h Informatio

GUIDELINES AND PRACTICES Manual

Alberta's Health INFORMATION Act

Alberta
HEALTH AND WELLNESS

102-01024/

Alberta's Health
INFORMATION
Act

Health Information Act

GUIDELINES AND PRACTICES

2001

Alberta
HEALTH AND WELLNESS

Introduction

This *Manual* provides a comprehensive reference tool for the application of the *Health Information Act* by all custodians that are subject to the *Act*.

This *Manual* is provided as information only and is intended to serve as a supplement to the *Health Information Act* and Regulation. The information contained in it is provided as guidelines, not as binding rules.

All best practices and examples used are provided as illustrations and should not be used as authority for any decisions made under the *Act*. This publication is not to be used as a substitute for legal advice. In case of any doubt as to the proper application of the *Act*, please consult with your Health Information Act Coordinator.

For further information about the use of the Guidelines and Practices Manual please contact:

Information Services Unit
Alberta Health and Wellness
15th Floor, 10025 Jasper Avenue
Telus Plaza North Tower
Edmonton, Alberta T5J 2N3
Phone: (780) 427-8089
Fax: (780) 422-5813
Web site: http://www.health.gov.ab.ca

HEALTH INFORMATION ACT

GUIDELINES AND PRACTICES MANUAL

Table of Contents

Chapter 1: Introduction.. 1

1.1 Purpose of the Manual... 1
1.2 Purposes of the *Health Information Act* 2
1.3 Introduction to the *Health Information Act*.................3
1.3.1 Principles Underlying the Legislation.........................3
1.3.2 How the *Act* Works.. 7
1.4 To What and To Whom Does the *Health Information Act* Apply?...9
1.4.1 To What Information Does the *Health Information Act* Apply?..9
1.4.2 To Whom Does the *Health Information Act* Apply...... 14
1.4.3 Distinguishing Between Requests for "Health Information" Under the *Health Information Act* and Requests for "Personal Information" Under the *FOIP Act*.. 16
1.5 Scope of the *Health Information Act* 16
1.5.1 What the *Health Information Act* Does Not Apply To.. 16
1.5.2 Other Matters Related to the Scope of the *Act*........... 17
1.6 Inconsistency or Conflict with Another Enactment...18

THINGS TO REMEMBER
Who and What is Subject to the Act?......................20

Chapter 2: An Individual's Access to Own Health Information... 25

2.1 Overview of Chapter Two..................................25
2.2 How Do Custodians that are also Public Bodies Under the *FOIP Act* Deal with Access Requests?....... 25
2.3 How Does an Individual Exercise the Right of

Access to the Individual's Own Health Information? 26
2.3.1 Existing Procedures Still Available 27
2.3.2 Nature and Form of Request 28
2.3.3 Right of Access Exercised by Individual or by the Individual's Authorized Representative 29
2.3.4 Right of Access to Disclosure Information 32
2.4 How Should a Custodian Respond to an Individual's Request for Access to the Individual's Health Information? 33
2.4.1 Duty to Assist Applicants 33
2.4.2 Creating a New Record 33
2.4.3 Time Limit for Responding to Request 34
2.4.4 Extending Time Limit 35
2.4.5 Payment of Fees 36
2.4.6 Deemed Request under the *FOIP Act* 37
2.4.7 Response to Applicant 38
2.4.8 Model Responses 38
2.4.9 Dealing with Repetitious or Systematic Requests 40
2.5 Administering the Request Process 41
2.5.1 Receiving and Logging the Request 41
2.5.2 Clarifying the Request 42
2.5.3 Acknowledging the Request 42
2.5.4 Locating and Retrieving Records 43
2.5.5 Copying Retrieved Records 44
2.5.6 Preliminary Assessment 44
2.5.7 Notices 45
2.5.8 Estimating, Assessing and Excusing Fees 46
2.5.9 Consulting with Others 49
2.5.10 Reviewing Records 49
2.5.11 Severing Information 51
2.5.12 Documenting and Tracking Requests 53
2.5.13 Maintaining Copies of Requests and Records 54
2.5.14 Closure and Retention of Request Files 54
2.6 Abandonment of Requests 55

THINGS TO REMEMBER

Access to An Individual's Own Health Information 56
Model *Health Information Act* Access Request

Chart 58

Chapter 3: Exceptions to Right of Access to Individual's Own Health Information 60

3.1 Overview of Chapter Three 60
3.1.1 Right of Access Subject to Specific and Limited Exceptions 60
3.1.2 Meaning of Harm 61
3.1.3 Revealing a Class of Records 62
3.1.4 Exercising Discretion 62
3.1.5 Application of Exceptions and Response to Applicant.. 63
3.2 Relationship to Other Acts 63
3.3 Discretionary Exceptions 64
3.3.1 Disclosure Expected to Harm or Threaten the Applicant's or Another Individual's Mental or Physical Health or Pose a Threat to Public Safety 64
3.3.2 Disclosure Leading to Identification of a Confidential Source of Health Information 67
3.3.3 Disclosure Revealing Advice Developed by or for or Consultations Involving a Member of Executive Council 70
3.3.4 Disclosure Revealing Advice Developed by or for Regional Health Authorities or Provincial Health Boards 74
3.3.5 Disclosure Prejudicing Use or Results of Audits, Diagnostic Tests or Assessments 76
3.4 Mandatory Exceptions 78
3.4.1 Disclosure of Information about an Individual Other Than the Applicant 78
3.4.2 Disclosure of Procedures or Results of an Investigation Of a Health Services Provider 80
3.4.3 Disclosure Revealing Substance of Deliberations of Executive Council or Treasury Board 82
3.4.4 Disclosure Prohibited by Another Enactment of Alberta 87

THINGS TO REMEMBER
Right to Refuse Access to Health Information 90

Chapter 4: Correction or Amendment of Health Information....92

4.1 Overview of Chapter Four....................................92
4.2 How Does an Individual Request a Correction to or Amendment of the Individual's Health Information?... 92
4.2.1 Nature and Form of Request.............................. 93
4.2.2 How Does a Custodian Respond to a Request for Correction or Amendment of Health Information?...... 93
4.2.3 Agreeing to Make a Correction or Amendment..........93
4.2.4 Refusing to Make a Correction or Amendment.......... 94
4.2.5 Time Limits for Responding.............................. 96
4.2.6 Extending Time Limits......................................96
4.2.7 Deemed Requests for Correction or Amendment under the *FOIP Act*..98
4.3 Administering the Correction or Amendment Process.. 99
4.3.1 Receipt and Logging of Request.......................... 99
4.3.2 Clarifying the Request......................................99
4.3.3 Acknowledging the Request................................99
4.3.4 Locating and Retrieving Records........................ 100
4.3.5 Copying Retrieved Records............................. 100
4.3.6 Reviewer's Recommendations........................... 101
4.3.7 Documenting and Tracking Requests for Correction or Amendment.. 101
4.3.8 Maintaining Copies of Requests and Records..........102
4.3.9 Closure and Retention of Request Files................ 102
4.3.10 Abandonment of Requests............................... 103

THINGS TO REMEMBER
Correction or Amendment of Health Information......104

Chapter 5: Duties and Powers of Custodians Relating to Health Information.. 106

5.1 Overview of Chapter Five.................................. 106
5.2 General Duties of Custodians..............................106
5.2.1 Duty to Collect, Use and Disclose Health Information with the Highest Degree of Anonymity Possible...................................... 107

5.2.2 Duty to Collect, Use and Disclose Health Information in a Limited Manner 108
5.2.3 Duty to Obtain Consent Before Disclosing Diagnostic, Treatment and Care Information by Electronic Means 109
5.2.4 Duty to Protect Health Information 113
5.2.5 Duty to Ensure Accuracy of Health Information 122
5.2.6 Duty to Identify Responsible Affiliates 122
5.2.7 Duty to Establish or Adopt Policies and Procedures 123
5.2.8 Duty to Prepare Privacy Impact Assessments 123
5.3 Powers of Custodians 136
5.3.1 Power to Transform Health Information 136
5.3.2 Power to Enter Agreement with Information Manager 140
5.3.3 Power to Charge Fees 147
5.4 Data Matching Rules 147
5.4.1 General Prohibition Respecting Data Matching 148
5.4.2 Data Matching Within a Custodian 148
5.4.3 Data Matching Between Custodians 148
5.4.4 Data Matching Between a Custodian and a Non-custodian 149
5.4.5 Data Matching for Research Purposes 149

THINGS TO REMEMBER

Duties and Powers of Custodians Relating to Health Information 151
Consent Under Section 59 155

Chapter 6: Collection of Health Information 157

6.1 Overview of Chapter Six 157
6.2 Limits on Collection 157
6.2.1 Duty to Collect Health Information with Highest Degree of Anonymity 157
6.2.2 Duty to Collect Health Information in a Limited Manner 158
6.2.3 Applying the 'Need to Know' Principle to the Collection of Health Information by an Affiliate 159
6.3 Collecting Non-identifying Health Information 159
6.4 Authority to Collect Individually Identifying Health Information 159

6.5 Collecting Personal Health Numbers.................... 162
6.5.1 Right to Require Provision of Personal Health Number...162
6.6 Manner of Collection....................................163
6.6.1 Duty to Collect Directly from Individual................163
6.6.2 Authority for Indirect Collection..........................163
6.6.3 Notifying the Individual About the Collection..........168
6.7 Using a Recording Device...............................170

THINGS TO REMEMBER
Collection of Health Information........................... 171
Decision Flow Chart for Collection....................... 174

Chapter 7: Use of Health Information............................. 176

7.1 Overview of Chapter Seven............................... 176
7.2 Limits on the Use of Health Information................ 176
7.2.1 Duty to Use Health Information with the Highest Degree of Anonymity Possible............................ 177
7.2.2 Duty to Use Health Information in a Limited Manner. 178
7.2.3 Applying the 'Need to Know' Principle to the Use of Health Information by Affiliates............................ 178
7.2.4 Limits on the Use of Non-Recorded Health Information..179
7.3 Using Non-identifying Health Information.............. 179
7.4 Authority for Custodians to Use Individually Identifying Health Information......................... 179
7.4.1 Authorized Purposes..................................... 180
7.4.2 Additional Authorized Purposes for Custodians with Health System Mandates.................................. 184
7.5 Use of Personal Health Number by Persons Authorized by Regulation................................ 186

THINGS TO REMEMBER
Use of Health Information.................................. 187
Decision Flow Chart for Use.............................. 190

Chapter 8: Disclosure of Health Information..................... 192

8.1 Overview of Chapter Eight............................... 192

8.2 Limits on Disclosure of Health Information............ 192
8.2.1 Duty to Disclose Health Information with the Highest Degree of Anonymity Possible..................193
8.2.2 Duty to Disclose Health Information in a Limited Manner.. 194
8.2.3 Applying the 'Need to Know' Principle to the Disclosure of Health Information by Affiliates.........195
8.2.4 Limits on the Disclosure of Non-Recorded Health Information..196
8.2.5 Duty to Ensure Authorized Recipient.................... 196
8.3 Disclosure of Individually Identifying Health Information to the Subject of the Information...........197
8.4 Disclosure of Individually Identifying Health Information with Consent...................................197
8.4.1 Requirements for Consent................................ 198
8.4.2 Disclosure of Diagnostic, Treatment and Care Information for Organ Donations and Transplants With Oral Consent..199
8.4.3 Requirements for Revocation of Consent............... 200
8.5 Disclosure of Individually Identifying Diagnostic, Treatment and Care Information without Consent......200
8.5.1 Disclosure to Another Custodian for Authorized Purposes.. 201
8.5.2 Disclosure to a Person Providing Continuing Treatment And Care to the Individual................................201
8.5.3 Disclosure to Family Members or Those in a Close Personal Relationship....................................202
8.5.4 Disclosure to Family Members Where Individual is Injured, Ill or Deceased................................ 202
8.5.5 Disclosure to Official of a Penal or Other Custodial Institution..202
8.5.6 Disclosure to a Person Authorized to Conduct an Audit...203
8.5.7 Disclosure to a Quality Assurance Committee..........203
8.5.8 Disclosure for the Purpose of a Court Proceeding...... 204
8.5.9 Disclosure for the Purpose of Complying with a Subpoena, Warrant or Court Order.................... 204
8.5.10 Disclosure to Police Investigating an Offence Involving a Life-threatening Personal Injury to the Individual...206

8.5.11 Disclosure to Another Custodian to Detect or Prevent Fraud or Limit Abuse of Health Services 208
8.5.12 Disclosure to an Officer of the Legislature 209
8.5.13 Disclosure to Avert or Minimize Imminent Danger to Health or Safety of Any Person 209
8.5.14 Disclosure in the Best Interests of an Individual Who Lacks the Mental Capacity to Provide Consent 210
8.5.15 Disclosure to a Descendant of a Deceased Individual, an Authorized Representative or Person Providing Health Services to a Descendant 211
8.5.16 Disclosure Authorized or Required by an Enactment of Alberta or Canada 212
8.5.17 Disclosure to the Successor of a Custodian 213
8.5.18 Disclosure to a Health Professional Body 214
8.6 Maintenance of Information on Disclosure of Individually Identifying Diagnostic, Treatment and Care Information 215
8.7 Notification of Recipient of Purpose and Authority For Disclosure of Diagnostic, Treatment and Care Information 216
8.8 Disclosure of Individually Identifying Diagnostic, Treatment and Care Information by Electronic Means. 216
8.9 Disclosure of Registration Information Without Consent 217
8.10 Disclosure of Health Services Provider Information Without Consent 218
8.11 Disclosure of Individually Identifying Health Information without Consent to an Archives 219
8.12 Disclosure by Minister or Department 219
8.13 Disclosure to Minister 220
8.14 Disclosure for Health System Purposes 220
8.14.1 Disclosure to Minister and Department 220
8.14.2 Disclosure to RHA's, Alberta Mental Health Board, Alberta Cancer Board 221
8.15 Disclosure for Research Purposes 223
8.15.1 Submission of a Research Proposal to an Ethics Committee 223
8.15.2 Role of Ethics Committee 224
8.15.3 Application to Custodian for Disclosure for Research Purposes 227

8.15.4 Agreement with Researcher ... 227
8.15.5 Consent for Additional Information ... 229
8.15.6 Court Order ... 229

THINGS TO REMEMBER

Disclosure of Health Information ... 231
Fundamentals of Consent ... 236
Decision Flow Chart for Disclosure ... 243
Decision Flow Chart for Disclosure for Health System Purposes (Section 46) ... 246
Decision Flow Chart for Disclosure for Health System Purposes (Section 47) ... 248

Chapter 9: Administration of the Act ... 250

9.1 Overview of Chapter Nine ... 250
9.2 Roles and Responsibilities ... 250
9.2.1 Custodians ... 250
9.2.2 Affiliates ... 251
9.2.3 Health Professional or Other Regulatory Bodies ... 251
9.2.4 Minister Responsible for the *Health Information Act* .. 251
9.2.5 Alberta Health and Wellness ... 251
9.2.6 Information and Privacy Commissioner ... 252
9.3 Identifying Responsible Affiliates ... 252
9.4 *Health Information Act* Implementation ... 252
9.5 Health Records Management or Information Management and Information Technology Functions. 255
9.6 Establishing or Adopting Policies and Procedures ... 256
9.7 Manner of Giving Notice ... 257
9.8 Liabilities, Sanctions and Penalties ... 257
9.8.1 Immunity from Suit ... 257
9.8.2 Protection of Employee ... 258
9.8.3 Offences and Penalties ... 258

Chapter 10: Commissioner's Powers and Duties ... 260

10.1 Overview of Chapter Ten ... 260
10.2 Appointment ... 260
10.3 Mandate and General Powers ... 261
10.4 Monitoring Role ... 262

10.5 Provision of Advice........264
10.6 Disclosure to the Commissioner........264
10.7 Powers to Conduct Investigations or Inquiries........264
10.8 Access to Information........265
10.9 Authorizing Custodians to Disregard Requests........265
10.10 Statements Provided to the Commissioner........266
10.11 Protection from Liability........266
10.12 Delegation of the Commissioner's Powers........267
10.13 Reviews and Investigations........267
10.14 Adjudicator Process........273
10.15 Judicial Review........274

Chapter 11: Records and Information Management, Privacy And Security........277

11.1 Overview of Chapter Eleven........277
11.2 Records and Information Management........277
11.2.1 Powers of the Commissioner........278
11.2.2 Records Issues Relating to Access Requests........278
11.2.3 Records and Information Management Principles........282
11.2.4 Records and Information Management Policy Components........283
11.3 Privacy, Information Management and Security........288
11.3.1 Reviewing Compliance with Parts 3 to 6 of the *Act*........288
11.3.2 Review of Forms........296
11.3.3 Conducting a Threat and Risk Assessment........299
11.3.4 Developing a Security Policy........301

Chapter 12: Consequential Amendments........306

12.1 Overview of Chapter Twelve........306
12.2 Introduction to Paramountcy as it Applies to the *Health Information Act*........306
12.3 Relationship with the *FOIP Act*........307
12.4 Confidentiality Provisions in Other Statutes Now Governed by the *Health Information Act*........307
12.5 Statutory Provisions that Prevail over the *Health*

Information Act.. 310
12.6 Statutory Provisions that Maintain the Status Quo..... 312
12.7 Housekeeping Amendments..............................312

Appendix to Chapter 12 – Full Text of the *Health Information Act* Consequential Amendment and the Legislative Provision that was Amended.. 314

Appendixes:

Appendix 1: ***Health Information Act* Forms**
Appendix 2: **Model Letters**
Appendix 3: **Responsibilities of Custodians and the *Health Information Act* Implementation Checklist**
Appendix 4: **Components for Agreements under the *Health Information Act***

Index:

CHAPTER ONE

INTRODUCTION

This Chapter will cover:

- the purpose of the *Manual*;
- the purposes of the *Health Information Act;*
- a brief overview of the *Health Information Act,* including the principles underlying the legislation and how the *Act* works;
- to what and to who the *Health Information Act* applies to; and
- distinguishing between access requests under the *FOIP Act* and the *Health Information Act.*

1.1 PURPOSE OF THE MANUAL

The *Health Information Act* and the regulations made under it establish the rules that must be followed for the collection, use, disclosure and protection of health information. The *Health Information Act Guidelines and Practices Manual* is designed as a reference tool to help custodians and affiliates apply and administer the *Act.*

The *Manual* is intended to explain the legislation and to offer guidance on approaches, procedures and best practices. The information contained in the *Manual* is not meant to present binding rules. Any examples used are illustrative only and should not be used as authority for any decisions made under the *Act.*

The chapters of the *Manual* generally follow the scheme and order of the *Act.* A few chapters have been added to cover administrative processes and the first chapter is an overall introduction to the *Act.* At the back of many of the chapters are *'Things to Remember'*. These pages include bullet summaries of the important things to remember in the preceding chapter and, in some cases, decision flow charts or tables. They are meant to be used by readers as quick reminders or checklists about a particular topic but are not meant as a substitute for the more comprehensive chapter content or for referring to the *Act* and the regulations.

The *Act* and regulations can be found at: http://www.gov.ab.ca/qp

There are a number of Appendices at the back of the *Manual.* These include forms, model letters, a detailed implementation checklist and components for agreements under the *Act.*

Best practices used in the *Manual* should be considered as guidelines only. They are italicized in boxes accompanying the text.

References to Orders or Practice Notes from the Office of the Information and Privacy Commissioner (OIPC) should also be considered as guidelines only since they are based upon reviews, investigations and practices related to the *Freedom of Information and Protection of Privacy (FOIP) Act,* not to the *Health Information Act.*

Health Information Act and *FOIP Act* Orders will be distinguished by their numbering in the Commissioner's Office. That office will also develop separate *Health Information Act* Practice Notes, where needed.

For information about the Office of the Information and Privacy Commissioner, see the Website for the Office at:
http://www.oipc.ab.ca

Portions of the *Manual* have been adapted from the *Freedom of Information and Protection of Privacy Guidelines and Practices (2000)* published by Information Management and Privacy Branch of Alberta Municipal Affairs. We gratefully acknowledge this contribution.

For information about the *FOIP Act,* see the Website for Information Management and Privacy Branch at:
http://www.gov.ab.ca/foip

In case there is any doubt as to the proper application of the *Act,* readers should request advice from the *Health Information Act* Coordinator (or the affiliate responsible for administering the *Act*) in their organization.

For further information about the administration or application of the *Act,* please contact:

Information Services Branch, Alberta Health and Wellness, 15th Floor, Telus Plaza North Tower, 10025 Jasper Ave., Edmonton, Alta. T5J 2N3, (780) 427-8089 (Tel), (780) 422-5813 (Fax).

The Website for Alberta Health and Wellness is:
http://www.health.gov.ab.ca

Throughout the *Manual* there are references to "Minister" and "department". These refer to the Minister of Alberta Health and Wellness or the Minister responsible for the *Health Information Act* and the department of Alberta Health and Wellness, respectively.

1.2 PURPOSES OF THE *HEALTH INFORMATION ACT*

The purposes of the *Act* are set out in **section 2.** They are:

- ***Establishing mechanisms for protecting the privacy of individuals and the confidentiality of their health information***
  To establish strong and effective mechanisms to protect the privacy of individuals with respect to their health information and to protect the confidentiality of that information;

- ***Enabling appropriate sharing and accessing of health information***
  To enable health information to be shared and accessed, where appropriate, to provide health services and to manage the health system;

- ***Prescribing rules for the collection, use and disclosure of health information***
  To prescribe rules for the collection, use and disclosure of health information, which are to be carried out in the most limited manner and with the highest degree of anonymity that is possible in the circumstances;

- ***Providing an individual with a right of access to the individual's own health information***
  To provide individuals with a right of access to health information about themselves, subject to the limited and specific exceptions as set out in the *Act*;

- ***Providing an individual with a right to request correction or amendment of the individual's own health information***

To provide individuals with a right to request correction or amendment of health information about themselves;

- ***Establishing remedies for contravention of the Act***
  To establish strong and effective remedies for contravention of the *Act;* and
- ***Providing for an independent review process***
  To provide for the Information and Privacy Commissioner to conduct independent reviews of decisions made by custodians under the *Act* and to investigate and resolve complaints.

1.3 INTRODUCTION TO THE *HEALTH INFORMATION ACT*

The basic objective of the *Health Information Act* is to make the rules about the collection, use and disclosure of health information transparent to those involved in the health system as well as to the general public. The rules are intended to protect the privacy of individuals and the confidentiality of their health information; ensure that health information is shared appropriately; and ensure that health records are managed and protected properly.

1.3.1 PRINCIPLES UNDERLYING THE LEGISLATION

- **Custodians are responsible for maintaining, protecting and safeguarding health information.**

A **"custodian"** is someone in the health system who receives and uses health information and is responsible for ensuring that it is protected, used and disclosed appropriately.

"Custodian" is defined in **section 1(1)(f)** to include organizations such as regional health authorities and provincial health boards; health service providers paid under the Alberta Health Care Insurance Plan (such as physicians); pharmacies and licensed pharmacists; and the Minister and department.

The definition of custodian does not include the Alberta Alcohol and Drug Abuse Commission (AADAC), Persons with Developmental Disability (PDD) Boards and ambulance attendants, as defined in the *Ambulance Services Act.* It also does not include other provincial government departments and agencies, local public bodies such as schools, post-secondary institutions and municipalities and other private sector entities.

- **Custodians are the trusted "gatekeepers" of an individual's health information.**

Custodians must determine whether the amount and type of information to be used and disclosed is necessary and appropriate to achieve an authorized purpose under the *Act*; whether they have authority to use or disclose the information; and whether any expressed wishes of the individual are considered before disclosure, along with other factors.

- **Individuals have the right to access their own health information, to ask for it to be corrected and to know why it is being collected.**

Individuals have a right to examine or review their own health information and to ask for copies, explanations, and corrections or amendments to be made to it.

When a custodian asks an individual for specific health information, the custodian must explain why the information is being collected, under what legal authority it is being collected and who the individual can contact if there are any questions.

Custodians are expected to make a notation every time a record containing individually identifying diagnostic, treatment or care information is disclosed without consent and to allow the individual in question to have access to this notation.

- **Personal health numbers of individuals are protected.**

Only custodians and others designated by a regulation under the *Act* can require an individual to provide their personal health number **(section 21). Section 5(2)** of the Health Information Regulation designates certain persons or organizations and the specific purposes for which they are authorized to require the provision of personal health numbers. Examples of those designated by the regulation include insurers for the purpose of facilitating the handling, assessing and payment of claims for benefits; the Workers' Compensation Board for the purpose of facilitating the handling, assessing and payment of claims for benefits; and persons, other than custodians, who provide health services to individuals for the purpose of seeking reimbursement for providing those services from the Alberta Health Care Insurance Plan.

An individual can refuse to give his/her personal health number to anyone who is not covered by **section 21** of the *Act*. However, an individual may continue to provide his or her child's personal health number to private daycare operators or babysitters.

- **There are limits on the collection, use and disclosure of health information.**

As an overall principle, only the least amount of information at the highest degree of anonymity can be collected, used and disclosed **(sections 57, 58).**

Custodians are expected to only collect, use and disclose essential information and, wherever possible, to do so in a way that does not identify an individual.

- **When health information identifies an individual, there are specific rules for its collection, use and disclosure.**

If the information is non-identifying information, that is, either individual anonymous information or aggregate information (about groups of individuals with common characteristics), custodians may collect, use and disclose that information for any purpose.

- **Individually identifying health information may be used by custodians for authorized purposes as set out in section 27.**

Those authorized purposes include such things as providing health services to the individual; determining whether an individual is eligible for services under the Alberta Health Care Insurance Plan and conducting investigations or practice reviews of health professionals. For a complete list of authorized purposes under **section 27, see section 1.3.2 of this Chapter and also section 7.4 in Chapter 7 of this Publication.**

In addition, the Minister and the department, regional health authorities, the Alberta Cancer Board and the Alberta Mental Health Board may use individually identifying health information for planning and resource allocation; health system management; public health surveillance; and health policy development within the geographic area in which they have jurisdiction to promote the objectives for which the custodian is responsible.

- **As a general rule, an individual's consent is required before individually identifying health information is disclosed (section 34).**

- **However, individually identifying diagnostic, treatment and care information may be disclosed without an individual's consent to the persons and for the purposes set out in sections 35, 38, 39, 40, 46 and 47.**

Some of those discretionary disclosures include disclosure to another custodian for a purpose listed in **section 27;** to a person responsible for giving continuing care to the individual; to family members or others with a close personal relationship, unless the individual expressly requests that family and friends not be informed; and to police investigating an offence involving a life-threatening injury to the individual, if not contrary to the expressed wish of the individual. This is not an exhaustive list.

- **Individually identifying registration information may be disclosed by a custodian without the individual's consent in the situations set out in sections 36, 38, 40, 46 and 47.**

Some of those discretionary disclosures include disclosure to any person for the purpose of collecting or processing a fine or debt owing by the individual to the Government or to a custodian; and disclosure for any of the purposes for which diagnostic, treatment and care information may be disclosed under **section 35(1) or (4).**

- **Individually identifying health services provider information may be disclosed by a custodian without the individual's consent in the situations set out in sections 37, 38, 40, 46 and 47.**

Some of those discretionary disclosures include a disclosure that is authorized or required by an enactment of Alberta or Canada; or disclosure to a health professional body if requested for the purpose of an investigation, a discipline proceeding or practice review relating to the health services provider.

- **Individually identifying registration information and diagnostic, treatment and care information may only be disclosed for research purposes by a custodian, without the individual's consent, under the conditions set out in Part 5 (Disclosure of Health Information), Division 3 (Disclosure for Research Purposes).**

Before individually identifying diagnostic, treatment and care information or registration information may be disclosed for research, the research proposal must have been assessed by an ethics committee designated by the Minister; the researcher must agree to comply with the conditions stated in **section 53;** and the researcher must enter into an agreement with the custodian to comply with the conditions set out in **section 54.**

- **There are special rules for the disclosure of health information by electronic means.**

A custodian intending to disclose individually identifying diagnostic, treatment and care information by electronic means must first ensure that the individual has consented to this form of disclosure **(section 59)**. **"Electronic means"** is defined in the **section 1(2)** of the Health Information Regulation to mean "a computer system that facilitates access by authorized persons to electronic or digital information that is stored in a computer database by a custodian."

The rules governing the disclosure of the least amount of information with the highest degree of anonymity apply to information stored and shared electronically. Custodians must have technical and physical safeguards in place to protect records and information in any form, including records and information collected and stored electronically.

- **There are rules for the disclosure by a custodian of individually identifiable health information to the Minister or department for health system purposes (section 46).**

Privacy impact assessments describing how the disclosure may affect the privacy of the individual subject must be submitted to the Information and Privacy Commissioner for comment before the information can be disclosed to the Minister or to the department.

- **There are rules for the disclosure by a custodian of individually identifying health information to the Alberta Mental Health Board, a regional health authority or the Alberta Cancer Board for health system purposes (section 47).**

One of the above custodians may request another custodian to disclose individually identifying health information for any of the purposes listed in **section 27(2)** under certain circumstances. For example, the requesting custodian may be authorized to obtain the information by an enactment of Alberta or Canada; or the information may relate to a health service provided by another custodian that is provided using financial, physical or human resources provided or administered by the requesting custodian.

If the disclosure is not authorized by another enactment of Alberta or Canada, the disclosing custodian may, under **section 47(2),** refuse to disclose the information if disclosure could result in immediate and grave harm to the subject of the information; could harm another individual or pose a threat to public safety. Any such dispute may be resolved by the Commissioner.

- **The Information and Privacy Commissioner plays a key role in providing an independent review and monitoring function under the *Act*.**

The Commissioner is responsible for reviewing decisions of custodians and affiliates under the *Act;* conducting investigations; providing advice; and resolving disputes.

- **There are penalties for breaking the rules for collection, use and disclosure of health information.**

It is an offence under the *Act* to collect, use, disclose or create health information in contravention of the *Act*. There are other offences set out in **sections 106** and **107** of the *Act*.

1.3.2 HOW THE *ACT* WORKS

"Custodians" of health information are individual health services providers or organizations that are primarily in the publicly funded health sector **(defined in section 1(1)(f)),** but are also private, licensed pharmacies and pharmacists, who have **"health information" (defined in section 1(1)(k))** in their custody or under their control. This information includes:

- **"diagnostic, treatment and care information"** (information about an individual's health and health services provided to the individual) **(section 1(1)(i)) ;**

- **"registration information"** (six categories including specified demographic information about an individual) **(section 1(1)(u)** of the *Act* and further defined in **section 3** of the Regulation)**;** or

- **"health services provider information"** (specified demographic, employment and professional information about health services providers working in the health system) **(section 1(1)(o)).**

Custodians are authorized to use **"individually identifying" (section 1(1)(p))** health information to carry out the purposes in **section 27 (1)** including:

- providing health services;
- determining an individual's eligibility to obtain health services;
- investigating, reviewing or inspecting the services provided by health service providers;
- conducting research into better health practices, services or management;
- providing health service provider education;
- carrying out specific purposes identified in other legislation (e.g. *Hospitals Act, Cancer Programs Act, Regional Health Authorities Act, Public Health Act*); and
- internal management, including: planning, resource allocation, policy development, quality improvement, monitoring, audit, evaluation, reporting, obtaining or processing payment for health services and human resource management.

Some custodians (the Minister and Department, regional health authorities, the Alberta Mental Health Board and the Alberta Cancer Board) are authorized to also use individually identifying health information for the purposes of:

- planning and allocating resources on a regional or provincial basis;
- managing the health system on a regional or provincial basis;
- conducting public health surveillance to determine and improve the health of the regional or provincial population; and
- developing health policies and programs on a regional or provincial basis **(section 27(2)).**

There is a boundary or **"controlled arena"** around the custodians who are subject to the *Act*. Subject to certain provisions in the *Act*, individually identifying health information can move from one custodian to another within that controlled arena for the authorized purposes in **section 27**. Outside the arena, the movement of individually identifying health information is more restricted.

Even within the **"controlled arena",** certain provisions in the *Act* create barriers that restrict the flow of health information. These provisions include:

- the duty of a custodian to consider the expressed wishes of an individual regarding the disclosure of individually identifying health information **(section 58(2))**;
- the need for the individual to consent to the disclosure of individually identifying health information **(section 34)** except for the discretionary disclosures in **Part 5 (Disclosure of Health Information)**;
- the duty of a custodian to collect, use or disclose individually identifying health information with the highest degree of anonymity possible **(section 57)**;
- the duty of a custodian to collect, use or disclose the least amount of individually identifying health information **(section 58)**;
- the duty of an affiliate to collect, use or disclose health information in a manner that is in accordance with the affiliate's responsibilities as determined by their custodian ('need to know' basis) **(sections 24, 28, 43)**;
- the duty of a custodian to protect the confidentiality of health information **(section 60)**;
- the need for an individual to provide consent before his or her individually identifying diagnostic, treatment and care information is disclosed by "electronic means" **(section 59)**;
- the need for custodians to prepare privacy impact assessments **(sections 46, 64, 70, 71 and 72)**;
- the duty of a custodian to make notations of disclosures of records of individually identifying diagnostic, treatment and care information without consent **(section 41)**;
- the Commissioner's power to make orders **(section 80)**; and
- offences and penalties that apply to custodians, affiliates and, in some cases, to all Albertans **(section 107)**.

The *Act* recognizes the need to disclose health information beyond the controlled arena to, among others:

- any person providing continuing treatment and care to the individual;
- the individual, the individual's authorized representative or others with the individual's consent;
- a professional body, auditor and quality assurance committee;
- a researcher, under certain conditions;
- those requiring information as outlined in other legislation;
- the court or a quasi-judicial body;
- any person to comply with a subpoena, court order or warrant;
- an Officer of the Legislature to perform his or her duties;
- any person to avert or minimize an imminent danger to the health or safety or any person;
- the police to investigate an offence involving a life-threatening injury to the individual;
- any person to act in the best interests of an individual who lacks the mental capacity to provide a consent; and
- family members, those with close personal relationships and descendents for specified purposes and under certain conditions.

For disclosure outside the controlled arena, the same rules apply. For instance:

- the custodian must act as the trusted gatekeeper of the information;
- informed consent and expressed wishes of the individual must still be considered;

- the custodian must only disclose the least amount of information at the highest degree of anonymity;
- the custodian must protect the information while it is in transit to the recipient of the information, even if that recipient is in another province or country; and
- the custodian must make a notation of disclosure without consent of a record containing individually identifying diagnostic, treatment and care information.

There are also some additional requirements that apply to disclosure by a custodian of individually identifying health information outside the controlled arena. The custodian must:

- notify the recipient of the custodian's authority to disclose and the purpose of the disclosure;
- take steps to ensure that the person who will receive the information is the person intended and is authorized to receive it; and
- ensure that a researcher submits the research project for review by an approved ethics committee and to comply with the requirements of the committee.

Recipients of health information both inside and outside the controlled arena are:

- prohibited from using the information for direct commercial marketing or fundraising purposes without consent;
- prohibited from taking steps to re-identify an individual from non-identifying information without first notifying the Information and Privacy Commissioner; and
- prohibited from requiring a person to provide their Personal Health Number, unless they are on an approved list in the Regulations and do not use it for additional purposes.

1.4 TO WHAT AND TO WHOM DOES THE *HEALTH INFORMATION ACT* APPLY?

The *Act* applies to **"health information"** about an individual that is collected, used or disclosed by **"custodians"** and **"affiliates"**, primarily in the publicly funded health system.

1.4.1 TO WHAT INFORMATION DOES THE *HEALTH INFORMATION ACT* APPLY?

The *Act* applies to **"health information"** about an individual. **"Health information"** includes any or all of the following three types of information: **(section 1(1)(k))**

- **"diagnostic, treatment and care information" (section 1(1)(i));**
- **"health services provider information" (section 1(1)(o));** or
- **"registration information" (section (1)(u)).**

"Diagnostic, treatment and care information" is the most sensitive information about an individual's health and the health services provided to that individual, including the cost of those services. The most stringent rules in the *Act* apply to this category of health information.

A custodian may only disclose individually identifying diagnostic, treatment and care information to a person other than the individual who is the subject of the information (or their authorized representative) if the individual (or their authorized representative) has consented to the disclosure. There are some exceptions to consent when disclosure of the information is for the purposes set out in **sections 35 (1) through (4), 46 and 47.**

Diagnostic, treatment and care information includes the following:

- information about the physical and mental health of an individual;
- a **"health service" (as defined in section 1(1)(m))** provided to an individual that is directly or indirectly and fully or partially paid for by the department for the purposes of:
    - protecting, promoting or maintaining physical and mental health;
    - preventing illness;
    - diagnosing and treating illness;
    - rehabilitation;
    - caring for the health needs of the ill, disabled, injured or dying; or

  provided to an individual by a pharmacist engaging in the practice of pharmacy as defined in the *Pharmaceutical Profession Act*, regardless of how the service is paid for;
- donation by an individual of a bodily part or substance, including information derived from the testing or examination of a body part or bodily substance;
- a drug as defined in the *Pharmaceutical Profession Act* provided to an individual;
- a health care aid, device, product, equipment or other item provided to an individual pursuant to a prescription or other authorization (such as Alberta Aids to Daily Living program);
- the amount of any benefit paid or payable under the *Alberta Health Care Insurance Act* or any other amount paid or payable in respect of a health service provided to an individual;

and includes any other information about an individual that is collected when a health service is provided to the individual but does not include information that is not written, photographed, recorded or stored in some manner in a record.

An example of **"other information collected"** would be certain information about an individual's authorized representative under **section 104(1)(c) to (i)**. Because the role of a parent or guardian of a child or guardian or trustee of an individual under the *Dependant Adults Act* is inextricably linked to the individual's diagnostic, treatment and care information, the name, address, phone number, signature etc. of that representative could also be included as diagnostic, treatment and care information. When the consent of an authorized representative is required to provide health services to e.g. a minor, the demographic information of the minor's authorized representative is linked to the provision of that health service.

"Health services" provided to populations include public health and community health services such as health screening programs (e.g. breast cancer screening program) if these are fully or partially paid for by Alberta Health and Wellness.

"Directly paid for by the department" means that the services are paid for out of the Alberta Health Care Insurance Plan under the *Alberta Health Care Insurance Act* or otherwise directly paid for by the department. Examples of this are Alberta Aids to Daily Living Benefits, services provided by a physician who is paid under that *Act* on a fee for service basis; or laboratory tests conducted by the Provincial Laboratory.

"Indirectly paid for by the department" means that the services are paid for by the department but through other sources of departmental funding. For example, laboratory or x-ray services may be provided by a health authority or by an affiliate of a health authority out of departmental grants.

"Fully paid for by the department" means that the services are completely paid for by the department.

"Partially paid for by the department" means that the services are partially funded by the department with the remainder privately funded, such as chiropractic services.

"Donation of a bodily substance" could include organ donations, donation of blood or blood products tissue samples retained by the Alberta Cancer Board and laboratory specimens.

A **"health service"** does not include a service that is provided to an individual:

- by an ambulance attendant as defined in the *Ambulance Services Act.*

  An **"ambulance attendant"** is a person who is engaged or employed to attend to or transport patients in an ambulance. Health information collected, used or disclosed by ambulance attendants is subject to the *Ambulance Services Act* and the Confidentiality Regulation (Alta. Reg. 38/99) made under that *Act*. Demographic and other pre-hospital information collected by ambulance attendants continues to be governed by the above legislation. However, if that information is provided to a hospital upon arrival, it becomes part of the patient's health care record and is subject to the *Health Information Act*.

- by the Alberta Alcohol and Drug Abuse Commission (AADAC) under the *Alcohol and Drug Abuse Act.*

  Section 8 of that *Act* requires current and former employees of the Alberta Alcohol and Drug Abuse Commission to not disclose any information that names or identifies a client of the program, subject to certain exceptions. This section outlines a different concept than that of the "controlled arena" under the *Health Information Act* **(see discussion of this concept under How the Act Works in Section 1.3.2 of this Chapter).**

  Information in the custody or under the control of AADAC is subject to the access and privacy protection provisions of the *Alcohol and Drug Abuse Act* and the *Freedom of Information and Protection of Privacy Act.*

- by a Community or Facility Board (PDD Board) as those terms are defined in the *Persons with Developmental Disabilities Community Governance Act.*

  PDD Boards collect and create "care information" about individuals. The information is used for such purposes as determining an individual's level of functionality during intake. However, this information it is not used for any of the purposes listed as authorized purposes in **section 27** of the *Health Information Act.*

Information in the custody or under the control of PDD Boards is subject to the access and privacy protection provisions of the *Freedom of Information and Protection of Privacy Act.*

"Diagnostic, treatment and care information" only refers to recorded information. It **does not include** information that is not written, photographed, recorded or stored in some manner in a record **(section 1(1)(i)).**

"Health services provider information" means information about a health services provider (an individual who provides "health services" **(section 1(1)(n))**. The information is collected by employers and health professional bodies that regulate health providers. It is needed for workforce planning and to identify whether a provider's right to provide services has been suspended or cancelled. This type of health information includes:

- name;
- business and home mailing addresses and electronic addresses;
- business and home telephone numbers and facsimile numbers;
- gender;
- date of birth;
- unique identification number that is assigned to the provider by a custodian for the purpose of the operations of the custodian, and uniquely identifies the provider in relation to that custodian;
- type of provider and licence number (if one has been issued);
- date on which the provider became authorized to provide health services and the date, if any, on which the provider ceased to be authorized to provide health services;
- education completed, including entry level competencies attained in a basic education program and post-secondary educational degrees, diplomas or certificates completed;
- continued competencies, skills and accreditations, including any specialty or advanced training acquired after completion of the education and the dates they were acquired;
- restrictions that apply to the provider's right to provide health services in Alberta;
- decisions of a **"health professional body"**, or any other body at an appeal of a decision of a health professional body, pursuant to which the health services provider's right to provide health services in Alberta is suspended or cancelled or made subject to conditions, or a reprimand or fine is issued;
- business arrangements relating to the payment of the provider's accounts;
- profession;
- job classification;
- employment status;
- number of years of practice in the profession;
- employer; and
- municipality in which the provider's practice is located.

A custodian may only disclose individually identifying health services provider information without the consent of the individual who is the subject of the information for the purposes set out in **sections 37, 38, 40, 46 or 47.**

"Business card" information of a health services provider may be disclosed without consent, unless the disclosure could reasonably be expected to subject the provider to harm to his or her physical or mental health **(section 37(2) but note the exceptions for home address, telephone number and licence number)** .

A **"health professional body"** in **section 1(1)(l)** means a body that regulates the members of a health profession or health discipline under an Act (e.g. the College of Physicians and Surgeons of Alberta under the *Medical Profession Act* or a college of a health profession under the *Health Professions Act* once that act is proclaimed in force).

A custodian who uses the personal health number of a health services provider as the provider's "unique identification number" for the custodian's operations, should, in future, move towards using a different number for this purpose.

"The date on which the health services provider became authorized to provide health services" refers to the date on which the provider was licensed to provide professional services (such as a registered nurse or physiotherapist) and the date on which the provider received hospital privileges (such as physician privileges).

"Business arrangements relating to the payment of the health services provider's accounts" refer to such things as the arrangements under which the provider practices and the way in which the provider is paid. This could include self-employment, a partnership, professional corporation or physical therapy corporation, etc., and the accounts into which the payments are deposited.

"Health services provider information" only refers to recorded information. It **does not include** information that is not written, photographed, recorded or stored in some manner in a record **(section 1(1)(o))**.

"Registration information" means the basic information collected when individuals register to receive health services. It is primarily used to determine whether a person is eligible to receive health services in Alberta and for billing purposes. This type of health information includes the following categories:

- demographic information, including the individual's personal health number;
- location information;
- telecommunications information;
- residency information;
- health services eligibility information; and
- billing information, including an individual's account number.

The specific elements of each of the above categories are set out in detail in section 3 of the Health Information Regulation.

It is important for custodians not to disclose individually identifying registration information, including account numbers without consent of the individuals who are the subjects of the information, except for the purposes set out in **section 36 (a), (b) or (c).**

"Registration information" only refers to recorded information. It **does not include** information that is not written, photographed, recorded or stored in some manner in a record **(section 1(1)(u))**.

1.4.2 TO WHOM DOES THE *HEALTH INFORMATION ACT* APPLY?

The *Act* applies to **"custodians"** of health information primarily in the publicly funded health system, licensed pharmacies and pharmacists **and** to their **"affiliates"**.

A **"custodian" (section 1(1)(f))** includes:

- the board of an approved hospital as defined in the *Hospitals Act* other than one that is owned and operated by a regional health authority or established and operated under the *Cancer Programs Act* (e.g. a hospital operated by a voluntary organization such as Caritas);
- the operator of a nursing home as defined in the *Nursing Homes Act* other than a nursing home that is owned and operated by a regional health authority (e.g. homes operated by private or voluntary operators such as Extendicare (Canada) Inc. or the Good Samaritan Society);
- a provincial health board established by regulations under the *Regional Health Authorities Act* (e.g. the Alberta Mental Health Board);
- a regional health authority established under the *Regional Health Authorities Act;*
- a community health council as defined in the *Regional Health Authorities Act;*
- a subsidiary health corporation as defined in the *Regional Health Authorities Act*;
- the Alberta Cancer Board under the *Cancer Programs Act;*
- a board, council, committee, commission, panel or agency that is created by a custodian listed above if all or a majority of its members are appointed by, or on behalf of that custodian (e.g. a Hospital Services Utilization Committee).

  A committee under this provision **does not include** a committee that has as its primary purpose the carrying out of quality assurance activities within the meaning of section 9 of the *Alberta Evidence Act*. Quality assurance committees are appointed to study, assess or evaluate the provision of health services with a view to continual improvement of the quality of health care of the level of skill, knowledge and competence of health service providers;
- a health services provider paid under the *Alberta Health Care Insurance Plan* to provide health services. This includes physicians, chiropractors, dental surgeons, dental mechanics, opticians, optometrists, podiatrists and osteopaths but only for services paid under the *Plan*;
- a licensed pharmacy as defined in the *Pharmaceutical Profession Act;*
- a pharmacist as defined in the *Pharmaceutical Profession Act;*
- the department and the Minister;
- an individual or board, council, committee, commission, panel, agency or corporation designated in the regulations as a custodian.

Section 2 of the Health Information Regulation defines the following review or appeal panels as custodians:

- Alberta Aids to Daily Living Benefits and Extended Health Benefits Appeal Panels;
- Billing Practice Advisory Committee;
- Hospital Privileges Appeal Board;
- Mental Health Patient Advocate;
- Mental Health Review Panels in Calgary, Edmonton and Ponoka;
- MS Drug Review Panel;

- Out-of-Country Health Services Committee; and
- Out-of-Country Health Services Appeal Panel.

The definition of **"custodian" does not include:**

- the Alberta Alcohol and Drug Abuse Commission (AADAC);
- A Community Board or a Facility Board (PDD Board) as those terms are defined in the *Persons with Developmental Disabilities Community Governance Act.*

  The same rationale for excluding AADAC and P.D.D. Boards from the definition of "health service" applies to the definition of "custodian". See the discussion of these exclusions in the previous **section 1.4.1. in this Chapter;**
- the Workers' Compensation Board (WCB). The WCB continues to be subject to the *Freedom of Information and Protection of Privacy (FOIP) Act.* The collection, use and disclosure of health information about injured workers by WCB is governed by the *FOIP Act* and by the *Workers' Compensation Act.*

An **"affiliate" (section 1(1)(a))** includes:

- an individual employed by a custodian;
- a person who performs a service for the custodian as an appointee, volunteer or student or under a contract or agency relationship with the custodian; and
- a health services provider who has the right to admit and treat patients at a hospital as defined in the *Hospitals Act.*

The rules for collection, use and disclosure of health information by custodians also apply to their affiliates so custodians must ensure that their affiliates are aware of and follow the same rules.

For example, when ABC Benefits Corporation acts as an agent of the Minister in providing non-group supplementary health insurance plans, it is an **"affiliate"** of the Minister subject to the terms and conditions of its contract with the Minister.

Private clinics or organizations that contract with regional health authorities (e.g. Gimbel Eye Clinic) to provide health services would also be **"affiliates"**. However, only that part of their business that is covered by the contract would be subject to the *Health Information Act.*

BEST PRACTICE: *To avoid having to set up two separate record keeping and information management systems (one to comply with the Health Information Act and one to deal with all the other business of the affiliate) it may be simpler to follow the Health Information Act rules for all of the business of an affiliate, including the portion which does not fall under their contract to a health authority.*

This would also enable the affiliate to maintain an integrated file on patients so as to facilitate access for the individual to his or her entire health care record.

Health services providers such as physicians who have hospital admitting privileges are included in the definition of affiliate. Although a visiting or consulting physician may not have admitting privileges at a hospital, he/she could still be an **"affiliate"** if performing a service for a custodian under a contract or agency relationship **(section 1(1)(a)(ii)).**

The definition of **"affiliate" does not include:**

- an operator as defined in the *Ambulance Services Act;* or

- an agent as defined in the *Health Insurance Premiums Act* that collects premiums on behalf of the Minister of Alberta Health and Wellness.

Under **section 6**, custodians who collect, use or disclose health information **pursuant to another enactment** (such as the *Public Health Act)* are still bound to comply with the rules under the *Health Information Act* in terms of that collection, use or disclosure.

1.4.3 DISTINGUISHING BETWEEN REQUESTS FOR "HEALTH INFORMATION" UNDER THE *HEALTH INFORMATION ACT* AND REQUESTS FOR "PERSONAL INFORMATION" UNDER THE *FOIP ACT*

The definition of **"record"** under the *Health Information Act* **(section 1(1)(t))** is the same as the definition of **"record"** in the *FOIP Act* **(section 1(1)(q) of that *Act*).**

A **"record"** in both acts means a record of health information in any form and includes notes, images, audiovisual recordings, x-rays, books, documents, maps, drawings, photographs, letters, vouchers and papers and any other information that is written, photographed, recorded or stored in any manner; but does not include software or any mechanism that produces records **(section 1(1)(t)).**

However, **section 4(1)(p) of the *FOIP Act*** says that the *FOIP Act* does not apply to health information as defined in the *Health Information Act* that is in the custody or under the control of a public body that is a **"custodian"** as defined in the *Health Information Act.*

In the event that a custodian subject to both acts receives a request for access to an individual's personal information, the rules regarding access to information under the *Health Information Act* would apply to the individual's **"health information"** as that is defined in the *Health Information Act* and the rules regarding access to information under the *FOIP Act* would apply to the individual's other **"personal information"** as that is defined in the *FOIP Act.*

For example, if a visitor to a hospital was injured during an incident involving a scuffle with hospital security staff and was treated at that hospital, the visitor's diagnostic, treatment and care information as a patient of the hospital would be subject to the *Health Information Act* access rules. However, any other personal information about the visitor, collected or created by security staff as a result of the incident, would be subject to the *FOIP Act* access rules.

For a further discussion of this, see section 2.4.7 of Chapter 2 of this Publication.

1.5 SCOPE OF THE *HEALTH INFORMATION ACT*

1.5.1 WHAT THE *HEALTH INFORMATION ACT* DOES NOT APPLY TO

The *Act* does not apply to:

- **Non-health services provided by a custodian.**

Under **Section 1(2)**, where a **"custodian"** provides services that are not **"health services" (as defined in section 1(1)(m))**, the *Act* does not apply to that custodian in respect of those other services, nor to information relating to those other services.

For example, if a physiotherapist provides rehabilitation services to an individual that are completely paid for privately, or a private medical clinic performs eye surgery or an MRI that is not funded through a contract with a regional health authority, any health information that is collected, used or disclosed in relation to those services is not subject to the *Health Information Act*.

- **Other processes for access to an individual's own health information.**

The *Health Information Act* sets out a process for individuals to follow when they are requesting access to, or correction or amendment of, their own health information **(Part 2) (Individual's Right to Access Individual's Health Information)**. However, an individual is not limited to the procedure set out in that Part to request access to the individual's own health information if another procedure is available, provided it complies with the *Health Information Act* **(see section 2.3.1 in Chapter 2 of this Publication for examples of other processes).**

It is important to note that a person requesting access to another individual's health information would not make a request for access to health information under **Part 2** of the *Act* unless they were acting in a representative capacity under **section 104.** If they were not acting in a representative capacity for the individual, that kind of request would be subject to the disclosure provisions of the *Act* under **Part 5 (Disclosure of Health Information). See the discussion of this under section 2.3.3 Right of Access Exercised by Other Persons in Chapter 2 of this Publication.**

- **Collection of health information before the *Act* comes into force.**

Part 3 (Collection of Health Information) applies only in respect of health information collected after the *Act* comes into force. The parts of the *Act* dealing with use and disclosure of health information apply retroactive to the date of proclamation.

1.5.2 OTHER MATTERS RELATED TO THE SCOPE OF THE *ACT*

The *Act* does not:

- limit the information that would otherwise be available by law to a party to legal proceedings **(section 3(a)). "Legal proceedings"** are activities governed by the rules of court or rules of judicial or quasi-judicial tribunals that can result in a judgment of a court or a ruling by a tribunal.

  This means that the *Act* does not limit or prevent people from using legal processes such as examinations for discovery to gather information about a party in a lawsuit;

- affect the power of any court or tribunal to compel a witness to testify or to compel the production of documents; and

- prohibit the transfer, storage or destruction of a record in accordance with an enactment of Alberta or Canada. An "enactment" under the *Interpretation Act* is defined as an Act or regulation or any portion of an Act or regulation. This permits the orderly disposition of records by custodians in accordance with records retention and disposition schedules sanctioned by a law or regulation.

Section 108(1)(g) authorizes the Lieutenant Governor in Council to make regulations respecting the retention, disposal and archival storage of records for the purposes of **section 60 (Duty to Protect).** There are currently no regulations made under that section of the *Act*. There are, however, other acts and regulations governing retention and disposition, including the Operation of Approved Hospitals Regulation under the *Hospitals Act* and Regulations under the *Pharmaceutical Profession Act*.

Treatment of non-recorded health information

The *Act* applies to the three categories of **"health information"** in **section 1(1)(k);** namely, **"diagnostic, treatment and care information" (section 1(1)(i)); "health services provider information" (section 1(1)(o)); and "registration information" (section 1(1)(u)).** Those definitions specifically exclude information that is not written, photographed, recorded or stored in some manner in a record. However, a custodian may only use non-recorded (e.g. verbal) information for the purpose for which the information was provided.

1.6 INCONSISTENCY OR CONFLICT WITH ANOTHER ENACTMENT

Section 4 states that if a provision of the *Health Information Act* is inconsistent or in conflict with a provision of another Act or regulation, the provisions of the *Health Information Act* prevail unless

- another act, or
- a regulation under the *Health Information Act* expressly provides that the other act or regulation, or a provision of it, prevails over the *Health Information Act*.

A conflict or inconsistency may occur when access to information in another act is more restrictive than it is under the *Health Information Act*. For example, under the *Human Tissue Gift Act*, information about a recipient or donor cannot be disclosed. The conflict or inconsistency between the two acts has been resolved by making **section 11(1)** of the *Human Tissue Gift Act* prevail over the *Health Information Act*.

Conversely, a conflict or inconsistency may occur when the rules regarding disclosure of health information in the *Health Information Act* are more restrictive than a provision in another act, such as the *Child Welfare Act*. **Section 3** of that *Act* requires the reporting of information regarding a child in need of protection. **Section 4** of the Health Information Regulation expressly states that **section 3** of that *Act* prevails despite the *Health Information Act*.

On the other hand, a paramountcy provision is not needed where there is no conflict or inconsistency between a provision of the *Health Information Act* and a provision in another act. For example, if the right of a patient to obtain a copy of his or her medical records under the *Hospitals Act* is the same as the right of access to those records under the *Health Information Act,* there is no need to make one act prevail over the other.

There are no paramountcy issues between the *Health Information Act* and the *FOIP Act.* Health information in the custody or under the control of a public body (under the *FOIP Act)* that is also a custodian (under the *Health Information Act*) has been carved out or excluded from the *FOIP Act* **(section 4(1)(p))** of the *FOIP* Act). The right of access provisions and rules for collection, use, disclosure and protection of health information under the *Health Information Act* will apply to health information in the custody or under the control of custodians that are also public bodies.

Examples of other Paramountcies

After the *Act* is in force:

- disclosure of health information under the ***Mental Health Act*** or the ***Hospitals Act*** will be subject to the relevant provisions of the *Health Information Act* so those statutes will no longer be paramount over the *Health Information Act.*
- **section 20.11 of the *Cancer Programs Act*** will expressly state that **Part 1.1 of that *Act*,** dealing with the Cancer Registry, prevails over the *Health Information Act* if there is an inconsistency or conflict between that Part and the *Health Information Act.*
- **section 22(3) of the *Fatality Inquiries Act*** will expressly prevail over the *Health Information Act* to allow a medical examiner to inspect and make copies of any diagnosis, record or information relating to a person receiving diagnostic and treatment services in a diagnostic and treatment centre under the *Mental Health Act* or a patient under the *Hospitals Act.*
- **section 83 of the *Public Health Act*** will prevail over any enactment that it is in conflict or inconsistent with, including the *Health Information Act,* except for the ***Alberta Bill of Rights.*** A regulation under the ***Public Health Act*** prevails over any other by-law, rule, order or regulation with which it conflicts.

If there is a conflict or inconsistency between the *Health Information Act* and a provision of another act or regulation and there is no specific provision in the enactment or in the Health Information Regulation that states that the provision prevails over the *Health Information Act,* then decisions about access and disclosure must be made in accordance with the *Health Information Act.*

THINGS TO REMEMBER

WHO AND WHAT IS SUBJECT TO THE HEALTH INFORMATION ACT?

Who is Subject to the *Health Information Act*?

The *Health Information Act* primarily regulates individually identifying "health information" that is collected, used, disclosed and created by "custodians". To a lesser extent, it regulates non-custodians' collection, use and disclosure of individually identifying and non-identifying health information.

The *Act* applies to all individuals and organizations that are defined in the *Act* as "custodians" and "affiliates" of custodians. This includes all individuals and organizations that:

- provide health services that are funded in whole or in part, directly or indirectly, by the Minister;
- provide privately funded pharmacy and pharmacist services; and
- hear appeals or make decisions related to health services that are funded in whole or in part by the Minister;

The definitions of "custodian" and "affiliate" do not include the Workers Compensation Board, the Alcohol and Drug Abuse Commission, the Persons with Developmental Disabilities community or facility boards, ambulance operators and attendants, and agents of the Minister that collect health insurance premiums.

Who is a Custodian under the *Health Information Act*?

The *Act* defines the following individuals and organizations as **"custodians"**:

- the Minister;
- the department;
- regional health authorities (including the facilities operated by those authorities);

- the Alberta Mental Health Board (including the facilities operated by the board);
- the Alberta Cancer Board (including the facilities operated by the board);
- hospitals not owned or operated by health authorities (e.g. not-for-profit religious and voluntary hospitals);
- nursing homes not owned or operated by health authorities (e.g. not-for-profit religious and voluntary nursing homes and privately-owned for-profit nursing homes);
- community health councils of health authorities;
- subsidiary health corporations established by health authorities;
- boards, councils, committees, commissions, panels or agencies established by regional health authorities, the Alberta Mental Health Board, the Alberta Cancer Board, voluntary hospitals, voluntary or private nursing homes, community health councils and subsidiary health corporations;
- practitioners funded directly, in whole or in part, by the Alberta Health Care Insurance Plan (physicians, dental surgeons, dental mechanics, opticians, podiatrists, optometrists, chiropractors and osteopaths);
- licensed pharmacies and pharmacists; and
- an individual, board, council, committee, commission, panel, agency or corporation designated in the regulations as a custodian. To date, the regulation identifies the following additional custodians:

    - Alberta Aids to Daily Living Benefits and Extended Health Benefits Appeal Panels;
    - Billing Practice Advisory Committee;
    - Hospital Privileges Appeal Board;
    - Mental Health Patient Advocate;
    - Mental Health Review Panels (Calgary, Edmonton, Ponoka);
    - MS Drug Review Panel;
    - Out-of-Country Services Committee; and
    - Out-of-Country Health Services Appeal Panel.

The definition of custodian does not include other government departments, the Workers Compensation Board, the Alberta Alcohol and Drug Abuse Commission, the Persons with Developmental Disabilities community or facility boards, ambulance operators and ambulance attendants, agents of the Minister that collect health insurance premiums and any individual or organization that provides treatment and care

services that are totally privately funded (except pharmacists and pharmacies).

Who is an "Affiliate" of a Custodian?

The definition of **"affiliate"** includes:

- employees;
- any person that performs a service for a custodian as an agent, appointee, volunteer or student (i.e. any person that performs a service for the custodian -- there should be formal documentation that authorizes the person to perform the service); and
- hospital medical staff (i.e. physicians with hospital privileges) and other health care practitioners with formal access to hospital resources (e.g. midwives).

Agents acting on the behalf of the Minister for the collection of health insurance premiums (e.g. employers collect health insurance premiums) and ambulance operators are excluded from the definition of "affiliate".

What Information is Regulated under the *Health Information Act*?

Health information is regulated under the *Act*. **"Health information"** is defined as the following recorded information about individuals: diagnostic, treatment and care information, registration information and health services provider information. The reference to "recorded" is significant. The *Act* primarily regulates tangible records of information and not "non-recorded information". The *Act*, however, contains a few basic provisions to maintain the confidentiality of health information that is not recorded.

Diagnostic, Treatment and Care Information includes the following:

(i) the physical and mental health of an individual;
(ii) a health service provided to an individual;
(iii) the donation by an individual of a body part or bodily substance, including information derived from the testing or examination of a body part or bodily substance;
(iv) a drug as defined in the *Pharmaceutical Profession Act* provided to an individual;

(v) a health care aid, device, product, equipment or other item provided to an individual pursuant to a prescription or other authorization; and
(vi) the amount of any benefit paid or payable under the *Alberta Health Care Insurance Act* or any other amount paid or payable in respect of a health service provided to an individual;

and includes any other information about an individual that is collected when a health service is provided to the individual but does not include non-recorded information.

Registration Information includes information within the following general categories and is more specifically described in section 3 of the Health Information Regulation:

(i) demographic information (e.g. name, signature, personal health number, photograph, gender, date of birth, birth information, marital status, date of death, treaty status and whether the individual is a registrant or a dependant of a registrant under the *Health Insurance Premiums Act*);
(ii) location, residency and telecommunications information (e.g. home, business and mailing addresses, electronic address; health region; citizenship or immigration status; date of entry into Canada; province or country of birth or last residence; date of permanent residency; in the event a registrant or dependant under the *Health Insurance Premiums Act* is going to be absent from Alberta, such things as date of departure, forwarding address, etc.; and health service eligibility information); and
(iii) billing information (e.g. information about amounts owed, method of payment, individual's account number);

but does not include non-recorded information.

Health Services Provider Information includes information relating to a health services provider within the following general categories and is more specifically described in the *Act*:

(i) "business card" information (i.e. name, business address, electronic address, business telephone and facsimile numbers, type of health services provider, profession, job classification, employer and municipality in which the health services provider has practiced the profession);

(ii) demographic information;
(iii) employment and educational information; and
(iv) professional information.

Non-identifying Health Information means that the identity of the individual who is the subject of the information cannot be readily ascertained from the information. The *Act* primarily regulates information that identifies individuals, but not non-identifying information related to individuals. Non-identifying information includes statistical information about groups of individuals and anonymous individual information. The *Act* contains a few basic provisions restricting the use of non-identifiable information.

CHAPTER TWO

AN INDIVIDUAL'S ACCESS TO OWN HEALTH INFORMATION

2.1 OVERVIEW OF CHAPTER TWO

This Chapter will cover:

- how an individual can exercise the right of access to his or her own health information;
- how the right of access can be exercised by other authorized persons, on behalf of the individual;
- how a custodian should respond to a request for access to health information;
- how a custodian should administer the request process; and
- how a custodian may deal with abandoned requests.

2.2 HOW DO CUSTODIANS THAT ARE ALSO PUBLIC BODIES UNDER THE *FOIP ACT* DEAL WITH ACCESS REQUESTS?

Custodians subject to both acts need to be able to distinguish between requests for "health information" under the *Health Information Act* and requests for "personal information" under the *FOIP Act*.

In the event that a custodian subject to both acts receives a request for access to an individual's personal information, the rules regarding access to information under the *Health Information Act* would apply to the individual's **"health information"** as that is defined in the *Health Information Act* and the rules regarding access to information under the *FOIP Act* would apply to the individual's other **"personal information"** as that is defined in the *FOIP Act*.

For example, if a visitor to a hospital was injured during an incident involving a scuffle with hospital security staff and was treated at that hospital, the visitor's diagnostic, treatment and care information as a patient of the hospital would be subject to the *Health Information Act* access rules. However, any other personal information about the visitor, collected or created by security staff as a result of the incident, would be subject to the *FOIP Act* access rules.

"Personal information" is defined in **section 1(1)(n)** of the *FOIP Act* as recorded information about an identifiable individual, including

(i) the individual's name, home or business address or home or business telephone number,
(ii) the individual's race, national or ethnic origin, colour or religious or political beliefs or associations,
(iii) the individual's age, sex, marital status or family status,
(iv) an identifying number, symbol or other particular assigned to the individual,
(v) the individual's fingerprints, blood type or inheritable characteristics,
(vi) information about the individual's health and health care history, including information about a physical or mental disability,
(vii) information about the individual's educational, financial, employment or criminal history, including

criminal records where a pardon has been given,

(viii) anyone else's opinions about the individual, and

(ix) the individual's personal views or opinions, except if they are about someone else.

The definition in section 1(1)(n)(vi) includes information that would be considered "health information" under the *Health Information Act.*

"Health information" is defined in **section 1(1)(k)** of the *Act* as **"diagnostic, treatment and care information"; "health services provider information"; and "registration information"** as those terms are defined in the *Act.*

Note that the definition of "record" under the *FOIP Act* also includes "notes, images, audiovisual recordings and x-rays".

For a more detailed explanation of "health information" refer to section 1.4.1 in Chapter 1 of this Publication.

For a further discussion on how to deal with access requests if you are a custodian subject to both acts see section 1.4.3 in Chapter 1 of this Publication.

2.3 HOW DOES AN INDIVIDUAL EXERCISE THE RIGHT OF ACCESS TO THE INDIVIDUAL'S OWN HEALTH INFORMATION?

Under **section 7(1),** an individual has the right to access any record containing health information about the individual that is in the custody or under the control of a custodian.

This is similar to the right of access to information under the *Freedom of Information and Protection of Privacy (FOIP) Act* but, unlike the *FOIP Act,* the right only extends to health information about the individual and can only be exercised by the individual or the individual's representative **(see section 104).** The right of access **under section 7(1)** does not extend to someone other than the individual or the individual's representative.

To determine whether records are subject to *Health Information Act* for the purposes of **section 7(1),** it is not necessary for a custodian to have both custody and control of a record containing health information. There may be situations where a custodian has custody but not control of a record or vice versa.

See IPC Order 2000-005 for a discussion of this issue.

"Custody" means having possession of the health information or record containing health information and having the right to deal with the record or information.

"Control" means that a custodian has the authority to manage the health information or the record containing health information, in such ways as restricting, regulating and administering its use, disclosure or disposition.

Some indicators that a record may be in the custody or under the control of a custodian were set out in **IPC Order 99-032** and referred to in **IPC Order 2000-05.** The indicators mentioned in those orders were:

- the records were created by an officer or employee of the public body (read affiliate of the custodian), including an outside contracted consultant of the custodian;
- the records were specified in a contract as being under the control of a public body (custodian);
- the records were in the custody possession of the public body (custodian);
- the records were integrated with other records of the public body (custodian);
- the records related to the public body's (custodian's) mandate and functions;
- there were regulations regarding the use and disposition of the records; and
- the public body (custodian) has relied on the records to a great extent.

The most common situation where a custodian may have control, but not custody, of health information is in the case of contracted services. The information or record is created by and in the possession of the contractor, but the custodian has set out some rights of access to the records in its contract. For example, the contractor would have to furnish the custodian with information and particulars concerning the services provided and the care and progress of persons receiving the services.

In **IPC Order 2000-05,** the Commissioner found that, although the Calgary Regional Health authority did not have control over financial statements, contracts and other agreements related to Calgary Laboratory Services, it did have possession, and therefore, custody of the records. The records in question were thus subject to the *FOIP Act*.

Note that persons providing services for a custodian under a contract or agency relationship would be affiliates under **section 1(1)(a)**. As such, they could not contract out of their obligations and responsibilities under *Health Information Act*.

2.3.1 EXISTING PROCEDURES STILL AVAILABLE

As in the *FOIP Act*, under **section 17** of *Health Information Act*, if a custodian has another procedure available for individuals to access their own health information in certain situations, the individual may choose the existing process to access the information. This would allow for access without the formality and administrative expense of making a request under the *Act*.

The procedure set out in **Part 2** of the *Act* **(Individual's Right to Access Individual's Health Information)** may be used by individuals who have not been able to use existing procedures or who have not been satisfied with the amount or kind of information they have received through those procedures. There may be situations where confidence, trust or communication have broken down and individuals may prefer to request access to their health records using the process outlined in the *Act* and with the right of appeal to the Information and Privacy Commissioner.

The *Act* does not limit the information that would otherwise be available by law to a party to a legal proceeding **(section 3(a)).** This means that the *Act* does not prevent or limit the use of legal processes such as examination for discovery to gather information about a party in a lawsuit.

For example, a person may make a request to a custodian for health records relating to an individual involved in a civil or criminal legal action. If a lawyer is the authorized representative of an individual **(section 104)** and requests access to that individual's own health information, the request would be dealt with as a request under **section 7(1).** If a lawyer requests access to health information about someone other than his or her client, the request would be treated as a request for disclosure under **Part 5** of the *Act* **(Disclosure of Health Information).**

Once a legal action proceeds to discovery, or if some other legal procedure is invoked to obtain disclosure of records, the rules governing that legal procedure will apply. The access provisions of *Health Information Act* apply only to requests made under **Part 2** of the *Act* **(Individual's Right to Access Individuals' Health Information)** and not to other legal processes, although both processes may be happening at the same time.

The provisions of the *Act* do not override the power of any court or tribunal to compel a witness to testify or to compel the production of documents **(section 3(b)).**

Section 35(1)(i) facilitates those processes by permitting the disclosure of individually identifying diagnostic, treatment and care information for the purpose of complying with a subpoena, warrant or court order.

Note that the Fee Schedule in the Health Information Regulation does not apply to disclosures of health information under **Part 5** of the *Act* **(Disclosure of Health Information)**, such as disclosures to third parties like insurance companies. Custodians may charge their own fees for these services, for instance when a clinician has to create a new record or when records are copied and provided to third parties that are not custodians.

See Chapter 8 of this Publication for a more detailed discussion of the disclosure provisions of *Health Information Act.*

The right of access extends to all health information that is in the custody or under the control of the custodian, regardless of who created it or where it came from. For example, a health record containing health information created by a non-custodian that is in the custodian's files would potentially be accessible under the *Health Information Act.*

There are some exceptions to the right of access set out in **section 11 (See Chapter 3 of this Publication).** The right of access to a health record is subject to the payment of any fee required by the regulations **(section 7(3))** and any severing that may have to occur if any of the exceptions apply to the requested information.

2.3.2 NATURE AND FORM OF REQUEST

The provisions in the *Health Information Act* regarding the nature of a request are similar to those in the *FOIP Act.* **Section 8(1)** provides that an individual must make a request for access to the custodian that the individual believes has custody or control of the record.

Section 8(2) says that a custodian that has received a request for access to a record **may require** the applicant to submit the request in writing. This is different from the *FOIP Act* which requires all access requests to be in writing although there are provisions in the FOIP Regulation allowing applicants to make oral requests in certain circumstances.

An **"applicant"** is defined in **section 1(1)(b)** as the individual who makes a request for access under **section 8(1)** or a request for correction under **section 13(1).** An **"applicant"** is also an individual who makes a request for access to a record of notations of disclosure when the individual is the subject of that information **(section 41(3)).**

Custodians in small offices may decide to accept oral access requests. In order to manage the request process, larger custodians may require requests to be written. The exception may be for an applicant who cannot make a written request due to a language barrier or physical disability. However, custodians must still ensure that they deal with the access request in accordance with **sections 10, 11, 12, 15 and 16.**

Where a custodian requires requests to be submitted in writing, an applicant can use the **Request To Access An Individual's Own Health Information Form** found in **Appendix 1 of this Publication** or can simply write a letter requesting his or her own health information.

BEST PRACTICE: *Although a custodian may accept an oral request, if the custodian is large or decentralized, and especially if it is subject to both the FOIP Act and the Health Information Act, it would be better to require that all requests under section 7(1) be submitted in writing. This will enable the custodian to establish the starting date for the response time, provide clarity regarding the scope of the request and facilitate a request for records subject to the FOIP Act, if that Act applies to a portion of the request.*

Custodians should establish policies and procedures to deal with the acceptance of written and/or oral requests. The policies and procedures should address, among other things, the starting date for the response period. If the request is oral, it still needs to be documented and dated.

Applicants may ask to either examine the record requested or to obtain a copy of it **(Section 8(3)).**

2.3.3 RIGHT OF ACCESS EXERCISED BY AN INDIVIDUAL OR BY THE INDIVIDUAL'S AUTHORIZED REPRESENTATIVE

Section 104(1) states that any right or power conferred on an individual by this *Act* may be exercised by the following persons in certain circumstances. These rights or powers include the right to access an individual's own health information.

By the Individual Aged 18 or Over
(Section 104(1)(a))

An individual who is 18 years of age or older may exercise his or her own rights or powers under the *Act*.

By a Mature Minor
(Section 104(1)(b))

If the individual is under 18 years of age, and understands the nature of the right or power and the consequences of exercising the right or power, he or she may exercise that right or power. Even children younger than 12 years may be capable of understanding and making personal decisions or choices.

This provision leaves discretion in the hands of the custodian. Custodians should have a policy and procedure for dealing with minors based on the statutes and regulations under which they operate.

For example, provincial policy for community mental health clinics states that some factors to consider when deciding if a youth might emotionally and intellectually have the capacity to give consent are: maturity; economic status (i.e. self-supporting or not); living arrangements; mental state; risk assessment; and the complexity and intrusiveness of the treatment situation and treatment modality.

Similar factors might be helpful in determining whether a youth has the capacity to exercise the right of access to his/her own health information. The fact that a 14 year old girl seeks health care on her own may lead a custodian to believe that the girl might be considered a mature minor. The opinions and views of the minor are just one of the factors that must be taken into account in making a decision about who may exercise access rights. The custodian will also have to consider the context of each request to determine whether the right of access may be exercised by the minor or by a guardian.

Note that this category is not included in the *FOIP Act*.

By a Guardian of the Minor (Section 104(1)(c))

If an individual is under 18 years of age and the custodian determines that the individual does not understand the right or power and/or the consequences of exercising that right or power, the guardian must exercise the right or power.

A "guardian" is a person who has the care and custody of the minor or is involved in his or her daily care. This definition may not extend to the parents of a child in all circumstances. Other guardians may be a child's grandparent or other relative, the Director of Child Welfare or other individual who has been granted a temporary or permanent guardianship order.

By a Personal Representative of a Deceased Individual Over 18 Years (Section 104(1)(d))

If the individual is deceased and was 18 years of age or over immediately before death, the individual's personal representative (e.g. executor or administrator of the individual's estate) can exercise the right of access or other right or power of the individual under the *Act*.

However, the personal representative's right is limited to requesting health information or records that relate to the administration of the individual's estate. For instance, information in the individual's medical records at a physician's office about his/her health prior to death may be needed to assist the executor in a legal action related to the death and to the settlement of the estate.

Proof of the right to act on behalf of the deceased is normally a copy of the signed and attested document or a court document naming the representative to act in matters related to the estate. This would include, for example, a properly executed will or Letters of Administration from a court. Evidence that would not be sufficient would be an applicant's stated belief in his or her authority, whether by affidavit or statutory declaration, or evidence that an applicant administered the individual's estate in the past. **See IPC Order 98-004**.

The right of access for an individual who was under the age of 18 immediately before death would be exercised by the individual's guardian **(as in section 104(1)(c)).**

For information related to disclosure of health information to relatives of deceased persons, **see Sections 8.5.4 and 8.5.15 in Chapter 8 of this Publication.**

By a Guardian or Trustee Under the *Dependant Adults Act* (Section 104(1)(e))

If a guardian or trustee has been appointed for the individual under the *Dependant Adults Act,* the guardian or trustee may exercise the individual's rights provided the information requested relates to the powers or duties of the guardian or trustee. A trustee may need to access the results of certain tests conducted on a dependant adult to provide some evidence in court of the need to renew or terminate the guardianship order.

The document governing the nature of the guardianship or trusteeship provides the authority for the representative to act. Custodians should examine that document to ensure that the disclosure relates to the powers and duties stipulated in the document.

By an Agent of the Individual Under the *Personal Directives Act* (Section 104(1)(f))

If an agent has been designated under the *Personal Directives Act,* the agent can exercise the individual's rights. The disclosure is limited to the rights or powers given to the agent under the personal directive. Personal directives cannot provide authority over financial matters.

Custodians should examine the directive before disclosure. It may be necessary to access information about the capacity of the individual who made the directive or about the decision to be made by the agent in order to determine what information may be disclosed.

By an Individual Granted a Power of Attorney (Section 104(1)(g))

A power of attorney is an authority given to one person (called the attorney) to do certain acts in the name of, and personally representing, the person granting the power (called the donor). A power of attorney can be to perform specific acts on behalf of the donor or can be a general power of attorney to do everything that the donor can do. Some powers of attorney can be revoked by the donor. Some are irrevocable.

Some powers of attorney come into effect in the event of mental incapacity (e.g. an enduring power of attorney). Some remain in effect in the event of the mental incapacity of the donor, provided they comply with the provisions of the *Powers of Attorney Act*. The death of a donor normally revokes the power of attorney.
The exercise of the right or power under the *Health Information Act* must relate to the powers and duties conferred by the power of attorney. Information about the donor's physical or mental health may need to be accessed in order to determine whether a specified contingency has occurred that will bring the power of attorney into effect.

When the rights or powers conferred by the *Act* on an individual are to be exercised by someone holding a power of attorney, the custodian should verify the identity of the person holding the power of attorney and ensure that the power allows for the disclosure requested or any other power or right being invoked.

It may also be necessary, depending on the nature of the power of attorney, to verify that the donor is alive or that the donor is not suffering from a mental incapacity.

By the Nearest Relative of a Formal Patient under the *Mental Health Act* (Section 104(1)(h))

The **"nearest relative"** of a **"formal patient"** as defined in section 1(1)(d) of the *Mental Health Act* may exercise the right of access of an individual if the exercise of the right or power is necessary to carry out the obligations of the nearest relative under that *Act*.

A **"formal patient"** under the *Mental Health Act* means a patient detained in a facility on the basis of 2 admission certificates or 2 renewal certificates. **"Nearest relative"** is defined in **section 1(1)(h)** of that *Act*.

For certified (or formal) patients of various psychiatric facilities such as Alberta Hospital Edmonton, Alberta Hospital Ponoka and Claresholm Care Centre, or of hospital psychiatric wards at, for example, the University of Alberta or Foothills Hospitals, who do not have a legal representative or agent, the nearest relative may make specified decisions in the patient's best interest.

Note that this category of representative is not included in the *FOIP Act*.

By Any Person with the Individual's Written Authorization (Section 104(1)(i))

Any individual can provide authorization to another person to act on his or her behalf. Such authorization must be in writing, generally provide authority to the representative to exercise any right or undertake any power, including the right to provide consent under various provisions of the *Act*, or the right to access the individual's health information.

The authorization must be signed by the individual, and preferably witnessed. An example of an **Authorization of Representative Form** is included in **Appendix 1 of this Publication.**

Notices (Section 104(2))

This section provides that any notice required to be given to an individual under the *Act* may be given to the person entitled to exercise the individual's rights and powers referred to in **section 104(1).**

2.3.4 RIGHT OF ACCESS TO DISCLOSURE INFORMATION

Under **section 41(1),** custodians must make a notation each time they disclose without consent records containing individually identifying diagnostic, treatment and care information. The notation must describe the information and must indicate who the information was disclosed to, when it was disclosed and why.

An individual who is the subject of the information has the right to ask a custodian for access to such disclosure notations and for a copy of the information **(section 41(3)**. **Part 2 (Individual's Right of Access to Individual's Health Information)** applies to the request. Accessing this type of information does not have to be done by way of a separate request. Since disclosure notations would be placed on a patient's health record or be retrievable in a disclosure log by individual identifier, the information could be released to the individual as part of a request for access to all of their health information. Alternatively, if the disclosure notation is the only subject of the request, it could be processed as a separate request.

See Chapter 8.6 of this Publication for a further discussion of section 41.

2.4 HOW SHOULD A CUSTODIAN RESPOND TO AN INDIVIDUAL'S REQUEST FOR ACCESS TO THE INDIVIDUAL'S HEALTH INFORMATION?

2.4.1 DUTY TO ASSIST APPLICANTS

Section 10(a) expresses the duty of a custodian to make every reasonable effort to assist an applicant and to respond to each applicant openly, accurately and completely.

This means that if the applicant is not fully knowledgeable as to what records may exist or how they are organized, for example, the custodian has a duty to tell the applicant what they need to know in order for them to obtain as much of the information they are seeking as possible under the *Act*.

If there is an indication on an individual's health record that another custodian may also have health information about the individual, as part of the duty to assist, applicants should be advised that another custodian or other organization may have health information about them and that they may make a separate request to that custodian or organization.

This is an important duty to keep in mind throughout the request process. It is critical during the applicant's initial contact with a custodian. The Health Information Coordinator or person handling access requests under the *Act* should attempt to develop a working relationship with the applicant to define the nature and scope of the request and to determine the steps involved in processing the request.

2.4.2 CREATING A NEW RECORD

Under **section 10(b),** a custodian has an obligation to create a new record from an existing electronic record if:

- the record is in the custody or under the control of the custodian;
- the new record can be created using the custodian's normal computer hardware and software and technical expertise; and
- creating the record would not unreasonably interfere with the operations of the custodian.

This is the only case where the legislation requires a custodian to create a new record. It would be necessary to do this in a situation where the health information is stored in electronic or machine readable form and the custodian needs to create a human readable report or extract.

It is part of the custodian's duty to assist the applicant in locating the information which is the most useful and responsive to the request. The creation of a new record from manipulating data can be a considerable advantage to custodians in some instances. Information that is excepted from the record can sometimes be suppressed, saving long and tedious severing procedures.

The custodian should explain the methods used and what information is being suppressed so that the applicant does not think that information is being manipulated to alter the record or place a different perspective on it. Custodians should also take reasonable steps to ensure the information is accurate **(see IPC Order 99-014)**.

The provision is mandatory but extends only to the situation where the record can be created using its normal staff, equipment and software products, and where doing so would not unreasonably displace the business related data processing jobs necessary for the custodian to complete.

In determining whether creation of a record would unreasonably interfere with the custodian's operations, the person responsible for responding to the request should consult with both the medical records or other area that has the records as well as the information technology area to assess the time and resources which would be required to create the record and the impact which this use of resources would have on its day-to-day activities.

In addition to providing the record, under **section 10(c)**, the custodian must provide, at the applicant's request, and if reasonably practicable, an explanation of any term, code or abbreviation used in the record.

The duty to assist an applicant is limited by what is **"reasonably practicable"**. A custodian cannot be expected to fulfill this duty if the record was created by another custodian. A physician may not be able to personally provide an explanation. However, a health record technician or office nurse or other support person may be able to provide the assistance needed.

This section does not include an obligation to provide an explanation of the meaning or impact of the information contained in the records regarding the current or future health of the individual. However, if some of the information is illegible, the custodian should try to obtain a medical transcription of the information in the record or ask the health service provider to make the information legible before providing it to the applicant **(see IPC Order 98-002 – re illegible clinical notes as part of a Workers' Compensation Board claimant's access request).**

2.4.3 TIME LIMIT FOR RESPONDING TO A REQUEST

Section 12(1) provides that a custodian must make every reasonable effort to respond to a request within 30 days after receiving the request or within any extended period under **section 15.**

The 30 day limit is based on calendar days. The time period begins on the date the request is received in an office duly authorized to deal with it and, if applicable, any fee is paid. The short time period in which the *Act* requires a request to be processed emphasizes the usefulness of having a written request so that the starting date is clear.

If the request is incomplete and further information is required from the applicant, custodians should seek this information immediately. Such clarification does not alter the official date of receipt of the request. However, the need to seek more information may be grounds for extending the time limit.

Deemed Refusal

Section 12(3) clearly establishes that the failure of a custodian to respond to a request within the 30 day period or any extended period, is to be treated as a decision to refuse access to the particular record(s). Such action qualifies the request for complaint and review. In this case, the time limit for requesting a review by the Commissioner, under **section 74(2),** does not apply **(section 74(3)).**

2.4.4 EXTENDING TIME LIMIT

Section 15(1) sets out the only circumstances in which a custodian may extend the time limit for responding:

- where the request is vaguely worded or the record is impossible to locate without clarification from the applicant;
- where the search or review of a particularly large volume of records necessitates a longer response time and would unreasonably interfere with the operations of the custodian; and
- where the custodian consults with other custodians before deciding whether or not to grant access and cannot respond to the request within the time limit.

A custodian should consider all factors relating to the possibility of the need for a time extension before deciding to invoke one. Common factors include:

- the amount and type of detail needed from the applicant to clarify the request;
- the breadth and complexity of the request, the number of records requested and the number of files or sites which must be searched to find the requested records;
- the number and complexity of consultations required with other custodians or levels of government; and
- the quantity and type of records requiring review by other custodians.

Limits on Extensions

Custodians should make every effort to plan the processing of complicated requests so that there is a need to invoke only one extension. A custodian may, on its own authority and within the original 30 day time limit, extend the 30 day limit for up to 30 days, for a maximum of 60 calendar days.

If a custodian believes that responding to the request will require more than a total of 60 days, it is required to ask the Information and Privacy Commissioner ("the Commissioner") for permission to extend the time limit beyond the original 30 days. This must be done in writing and normally within the original 30 day time limit.

A letter to the Commissioner requesting the extension should set out the specific conditions relating to the request which will necessitate a period greater than 60 days for its processing and establish a reasonable period (e.g. 90 days) for producing a response.

In exceptional circumstances, a custodian who has already taken a 30 day extension, may seek a second extension from the Commissioner. This might occur when the relevant records suddenly involve complications not originally contemplated when planning the response process.

Where the Commissioner refuses to grant permission for an extension, the custodian has only a maximum of 60 days to process the request. Custodians must continue to process a request while awaiting the

Commissioner's response to an extension request.

Custodians must document the reasons for a time limit extension. This is required to support the custodian's decision to extend, for a request to the Commissioner for an extension of more than 30 days, and in the case of a complaint by the applicant to the Commissioner.

Notification

Section 15(2) requires the custodian to notify the applicant that an extension is being taken, the reason for it, the date when a response can be expected, and that the applicant has a right to make a complaint to the Commissioner about the extension.

Model Letter B in Appendix 2 deals with time extensions. This notice is required as soon as it is apparent that the request cannot be processed within the initial 30-day time period.

When a request for extension is made to the Commissioner, the notice should be sent to the applicant before the Commissioner's final decision on the extension has been made.

If an applicant complains to the Commissioner about an extension, the custodian continues to process the request throughout the review period.

After investigating a complaint about a time limit extension, the Commissioner may either confirm or reduce the extension of a time limit as provided in **section 80(3)(b).**

Day of Response

The Alberta *Interpretation Act* provides that, if the day a response is due falls on a statutory holiday or a day when the office of the custodian is closed, then the response is due on the next business day.

The custodian is responsible for determining whether the office that is authorized to respond is closed. If a small or single custodian's office is closed for staff vacations, the completion of the request will be affected and can legitimately be delayed until the first working day after the office reopens.

Larger custodians will need to establish policies and procedures to specify both the office that is authorized to receive requests and the hours during which that authorized office is open to receive requests. For example, although a Health Information Coordinator's office in a regional health authority may only be open Monday to Friday until 4:30 or 5:00 p.m, the health records area (where the records are stored) may be open 24 hours a day, 7 days a week.

2.4.5 PAYMENT OF FEES

An individual's right of access (under **Part 2** of the *Act*) to his or her own health information in a record is subject to the payment of any fee required by the regulations **(section 7(3)).** Custodians should collect all outstanding fees before releasing the records to the applicant.

The assessment of fees will also apply to oral requests unless the custodian excuses the applicant from paying all or part of a fee under **section 67(4).**

See the discussion on Estimating, Assessing and Excusing Fees under Section 2.5.8 of this Chapter.

2.4.6 DEEMED REQUEST UNDER THE *FOIP ACT*

If a written request for access to a record is made under **section 8(1)**, and the record contains information that would be subject to the *FOIP Act*, the part of the request that relates to that information is deemed to be a request under **section 7(1)** of the *FOIP Act* and that *Act* applies to that part of the request as if it had been made under **section 7(1)** of the *FOIP Act* **(section 16(1)**.

This section does not apply if the custodian that receives the request is not a "public body" as defined in section 1(1)(p) of the *FOIP Act*. The section would apply, for example, to a regional health authority, the Alberta Mental Health Board and the Alberta Cancer Board **(section 16(3))**.

The applicant must be notified regarding the part of the request that will be processed under the *FOIP Act* and whether this will affect the timelines for responding. **Model Letter A.1 of Appendix 2** can be used to notify applicants that part (or all) of the request is being deemed a FOIP Request under the *FOIP Act*. Since the provisions for processing access requests under the *FOIP Act* are very similar to those under *Health Information Act*, the impact of applying the *FOIP Act* to a part of the request should be minimal from the applicant's perspective.

BEST PRACTICE: *If the Health Information Coordinator for a custodian is a different person than the FOIP Coordinator, it will be important for the coordinators to consult with each other to discuss any difficult issues. However, the custodian will have to make its decisions regarding the release of records based upon the application of the act that applies to the relevant portion of the records.*

If the FOIP and Health Information Coordinators for the custodian are the same person, a separate file should be opened and a request number assigned for the part of the request that will be processed under the FOIP Act so that the steps taken to process the request can be properly documented. In the event that the applicant complains to the Commissioner or requests a review of a custodian's decision, this documentation will be important to support the procedures followed by the custodian or the decision(s) made in response to the request.

Section 14.1 of the *FOIP Act* has been amended so that if a request for access to a record is made under **section 7** of that *Act*, and a part of the record contains information to which *Health Information Act* applies, the part of the request relating to that information is deemed to be a request under **section 8(1)** of the *Health Information Act* and that *Act* applies to the processing of that part of the request.

This section does not apply if the public body that receives the request is not a custodian as defined in **section 1(1)(f)** of the *Health Information Act*.

Assessing Fees Where Both Acts May Apply

If a custodian that is also a public body under the *FOIP Act* (e.g. a regional health authority) receives a request from an individual to access the individual's personal information and the personal information includes health information (e.g. health information contained in incident reports or employee records), the deeming provisions in section 4.1 of the *FOIP Act* will apply. The *FOIP* Request would become two requests: one under **section 7(1)** of the *FOIP Act* and one under **section 8(1)** of *Health Information Act.*

The **Fee Schedule** in the FOIP Regulation would apply to the personal information requested, except for the portion of the records containing information to which the *Health Information Act* applies. The **Fee Schedule** under the Health Information Regulation would apply to the portion of the request related to health information.

BEST PRACTICE: *The individual has only made one request to access his or her information. Although custodians will process different portions of the request under the two Acts, they may wish to apply the lesser of the two fee schedules, where possible, unless the majority of the information requested is health information and significant review time will be required. Under the Health Information Act Fee Schedule, a fee may be charged for the time it takes to review and determine whether any severing will be required. Under the FOIP Act, a fee cannot be charged for this review time.*

Alternatively, the custodian could consider not assessing fees for a portion of the request.

2.4.7 RESPONSE TO APPLICANT

Section 12(2) provides that an applicant must be told:

- whether access to a record or part of it is granted or refused;
- if access to the record or part of it is granted, where, when and how access will be given, and
- if access to the record or part of it is refused:
    - the reasons for the refusal and the provision of the *Health Information Act* on which the refusal is based;
    - the name, title, business address and business telephone number of an affiliate who can answer the applicant's questions about the refusal; and
    - that the applicant may ask for a review of the decision by the Commissioner under **section 73(1).**

BEST PRACTICE: *When providing an applicant with access to his or her own personal information, a custodian must be satisfied that the individual receiving the information is, indeed, the individual the information is about or a duly appointed representative of that individual. For information on the exercise of rights by other persons, see* ***Chapter 2.3.3 of this Publication.***

Identification can usually be confirmed from the context of the request process, but where there is doubt, or the record contains diagnostic, treatment or care information, the custodian should request normal identification (e.g. photo identification such as a driver's licence) before providing the information. The identification only needs to be examined, not recorded (collected).

2.4.8 MODEL RESPONSES

Model Letters E, F and G in Appendix 2 of this Publication provide guidance and options for drafting the various types of final responses to the *Health Information Act* requests.

In all cases when access is denied, the response letter must state that, if the applicant requests a review of the decision by the Commissioner he or she should provide the Commissioner with:

- the request number assigned by the custodian;
- a copy of the decision letter; and
- a copy of the original request.

Generally, the response letter should address the outcomes of the search and review of records in response to a request.

Access is Provided

There is a determination that access will be provided because the information falls within the scope of the *Act*, and the information does not qualify for any exception under **section 11.** If it qualifies for a discretionary exception, the custodian has used its discretion in favour of releasing the information.

Some requests will involve records that take little time to review or are easily releasable. In these instances, the custodian should release available records as soon as possible rather than waiting until all records are ready for disclosure. This can occur when part of the request is deemed to be a request under the *FOIP Act* **(section 16(1))** or when the records contain information that requires further consultation. This situation could occur when some of the requested records were created by another custodian.

The applicant will have indicated, in accordance with **section 8(3),** whether he or she wishes to have a copy of the record or to examine the record. If the request is for a copy and it can be reasonably reproduced, the copy should be included in the response package. This will be done only if the fees have been paid.

If it is not possible to include the records, the applicant should be given the reason for the delay and told where, when and how the copy will be provided.

In some instances, the applicant may have asked to examine a record but the record cannot be reasonably severed for examination, or the record is in a format that does not readily lend itself to examination (e.g. a microfilm with much information on it that may be subject to exceptions under the *Act*). In these instances, the custodian may choose to provide a copy of the record to the applicant.

Access is Denied

Access is denied to all or part of a record if the information falls within a mandatory exception; the information falls within a discretionary exception and the decision is to deny access; or the information lies outside the scope of the *Act*. In these instances, the response provides:

- the reasons for refusal and the sections (specific subsections and paragraphs, where possible) on which the refusal is based;
- the name, title, business address and business telephone number of the custodian or affiliate, e.g. Health Information Coordinator, who will answer any questions the applicant may have about the response; and
- a statement that the applicant has the right to request a review of the decision under **section 73(1)** and that this request must be made within 60 days after the person asking for the review is notified

of the decision, or any longer period allowed by the Commissioner **(section 74(2)).**

2.4.9 DEALING WITH REPETITIOUS OR SYSTEMATIC REQUESTS

Under section 87, at the request of a custodian, the Commissioner may authorize the custodian to disregard one or more requests for access to or correction of the individual's own health information **(under section 8(1) or 13(1)).** The custodian must present facts in support of its request.

A custodian may be allowed to disregard a request or requests if:

- because of their repetitious or systematic nature, the requests would unreasonably interfere with the operation of the custodian or amount to an abuse of the right to make those requests, or
- one or more of the requests are frivolous or vexatious.

A request is **"repetitious"** if it is one in a series of requests by an applicant for substantially the same information or records.

Requests might be viewed as repetitious in cases where the applicant:

- continues to apply repeatedly for the same or similar information even though the original request has been disposed of and there is nothing new or different in the responsive records;
- continues to ask for corrections of particular opinions about him or herself when a decision has been made and the record has been annotated;
- makes the same request to a custodian before the previous request has been completed or any review or investigation procedure carried out.

A request is **"systematic"** in nature if it is part of an extensive pattern of related requests by an applicant or a group of applicants.

Requests might be considered systematic in nature when a single applicant (or a group of applicants) make(s) a large number of the same or similar requests; or regularly makes a request and then, after receiving a fee estimate, splits up the request into several separate requests to avoid fees.

A custodian may only request authorization to disregard repetitious or systematic requests if processing the request would unreasonably interfere with the operations of the custodian or amount to abuse of the right of access.

"Unreasonably interfere with operations" might be demonstrated by showing the impact that particular repetitious or systematic requests are having on the resources needed to respond within a custodian and the actual costs of providing a response.

"Abuse of the Right of Access" arises when the action of an applicant is demonstrably a misuse of the *Health Information Act.* It may be obvious that requests are not being made to obtain information or achieve a legitimate correction of information, but rather to tie up the resources of the custodian or frustrate the administration of a particular program or activity.

A request may be **"frivolous or vexatious"** if it has no sound basis in fact or is malicious. The applicant may not be making repeat requests or abusing his or her right of access under the *Act*, although that may be the case.

A custodian might support an argument that a request is frivolous or vexatious with reference to a past pattern of conduct that indicates an abuse of the process for access or with evidence that shows that the request is made in bad faith or for a purpose other than to obtain access to information.

Examples of requests that might be considered frivolous or vexatious include:

- continual requests for records that a custodian has already established it does not have;
- requests involving fees made by an applicant who has demonstrated a pattern of abandoning a request whenever a fee waiver is not granted or the Commissioner upholds a fee; or
- requests that show an intention to harass a public body, to "break" the system, or to engage in "information warfare".

When requesting the Commissioner's decision in such a case, the custodian might provide evidence of the considerable costs and time involved in dealing with a particular applicant or group of applicants.

No single factor will determine whether a request is frivolous or vexatious. Custodians need to present a case based on the history of requests by an applicant and the context of those requests, when asking for authority to disregard a request.

Asking for authorization to disregard requests should be rare. Custodians should ensure that they have fully discharged their duty to assist applicants in a full and forthright manner and have a strong case before seeking such authorization.

2.5 ADMINISTERING THE REQUEST PROCESS

Custodians should develop procedures to govern the processing of requests and to ensure that processing occurs within established time limits and in accordance with the requirements of the *Health Information Act.*

2.5.1 RECEIVING AND LOGGING THE REQUEST

Once a request is received by a custodian (this could be in the office of the Health Information Coordinator of a large or decentralized custodian or in the office of a single custodian), it should be registered and logged. This could be done electronically if an automated tracking system is in use.

It should then be placed in a request file and details of the request forwarded to any other office or program area of a custodian that has custody or control of the requested health record(s). In a regional health authority, for example, a request for all of a former patient's health information may have to be sent to several hospitals, contracted laboratory service providers, etc. The office of the affiliate that has been designated as responsible for processing access requests under the *Health Information Act* **(section 62(1))** can record the assignment of responsibility on the request tracking system.

Custodians may want to use an **Access Request Review Form (see Appendix 1 of this Publication)** to record all activities and the time involved in processing the request, in order to document the activities and assess the appropriate fees.

The identity of the applicant will be needed to locate and retrieve records containing the applicant's health information but should be disclosed only:

- to those officials and employees of the custodian who have a need to know it in order to carry out their job duties; and
- to the extent necessary to carry out the custodian's function in processing the applicant's request.

2.5.2 CLARIFYING THE REQUEST

A request may be overly general or vague because the applicant lacks knowledge of the custodian's operations or programs and the type of health records that may be available.

If a request does not sufficiently describe the records sought, a custodian should advise the applicant and offer to help clarify or narrow the request. **Model Letter A in Appendix 2** can be used in this situation.

If it appears from the health record that another custodian may have some or all of the records requested by the applicant, he or she should be notified of this and advised that he or she may make a separate request for that health information to the other custodian.

There are several things to keep in mind when trying to define or clarify a request.

Release of Information Outside the *Health Information Act*

If the information can be released through a more routine process, it should be released to the applicant without delay. However, any routine process for release must still comply with the rules in the *Act*. The applicant should be advised that such information is available without a request under the *Act* and that similar information can be obtained outside the *Act* in future. If only part of the information can be released in this routine manner, the rest of the request can be processed under the *Act*.

Narrowing a Request

If an applicant has requested a large amount of information that could result in significant fees being assessed, the Health Information Coordinator should try to narrow the request while still meeting the applicant's information needs. This could result in a reduction in fees and provision of better service, in terms of both time and results.

For example, narrowing the period of time over which the health information of an individual is sought, and specifying the health facilities within a regional health authority where the individual was a patient could reduce the search time and the amount of fees assessed.

If the scope of a request has been changed, the custodian should document the change and send a notice to the applicant **(see Model Letter A in Appendix 2).**

2.5.3 ACKNOWLEDGING THE REQUEST

The custodian should acknowledge receipt of a request. This acknowledgment may say that the request:

- has been received and processing will commence;
- is incomplete because the initial fee has not been paid and is required before processing can commence;

- is not clear or precise enough and more information is needed to clarify it before processing can commence; or
- if part of the request is deemed to be a request under the *FOIP Act*, how that part will be dealt with.

If processing cannot start immediately, an effort should be made to contact the applicant by telephone to resolve any problems quickly. A written follow-up to this call is good practice. It will provide a definite reference point as to when processing commenced.

Model Letter A in Appendix 2 sets out the options for acknowledging receipt of a request.

2.5.4 LOCATING AND RETRIEVING RECORDS

Under **section 10,** a custodian must make every reasonable effort to respond to an applicant openly, accurately and completely. Normally, the area responsible for the custody or control of records relevant to a request would be asked to locate and retrieve the records.

This responsibility may be delegated to the medical records technician or medical records unit of a health facility or clinic or it may rest with a staff member of a physician's or pharmacist's office. The retrieval of records would include any records that may reside in individual employee's offices, vehicles or homes, including electronic records, or in filing systems in storage areas. When applicable, records in the possession of contracted agencies may have to be located.

The support of records or information management staff may be needed to provide the indices and guides to appropriate records, where these are available, and to locate records.

Speed and accuracy are essential in identifying, locating, retrieving and, where appropriate, copying records relevant to a request. Where a request is for a large number of records, it may be appropriate that copies are not made immediately.

For a larger, decentralized custodian, a rule of thumb for a basic, uncomplicated request involving the coordination of staff in different areas is that four working days are needed to retrieve pertinent records that need to be reviewed.

Scope of Search

The *Act* applies to all health information, as defined in the legislation, including health information in electronic records, in the custody or under the control of the custodian. All records, in any form, that are responsive to the request, must be located and retrieved.

All areas where records are held – central active files, working files in individual offices, electronic repositories and off-site storage areas – must be searched and staff requested to produce relevant records, in accordance with the nature of the request. Any relevant records in the possession of contracted agencies and under the control of the custodian will have to be located, copied, if appropriate, and transferred to the Health Information Coordinator or individual processing the request.

An applicant can ask the Information and Privacy Commissioner to review the adequacy of a search to locate records **(section 85(a))**. When this happens, the custodian will have to demonstrate that it made a reasonable search of all areas and repositories where records relevant to the request might be located. **See IPC Order 96-022** for the criteria the Commissioner uses in judging the adequacy of a search for records.

Custodians must not dispose of any records relating to a request after it is received, even if the records are scheduled for destruction under an approved records retention and disposition schedule.

This includes any E-mail and transitory records relevant to the request that may exist at the time the request is received. The receipt of a request under **section 7(1)** freezes all disposition action relating to the records covered by the request until the request has been completed and any appeal to the Commissioner decided.

When a request is transmitted to the area or individual responsible for the records, the area or individual should be reminded that it is an offence to knowingly destroy any record **(section 107(1)(b))** or to alter, falsify or conceal any record, or to direct another person to do so **(section 107(1)(b)),** in order to evade a request for access to the record. These offences are punishable by a fine of up to $50,000.

Where records have been destroyed prior to the receipt of a request, in accordance with an approved records retention and disposition schedule, the custodian's response to the applicant should indicate that the records have been destroyed, quoting the authority for, and date of destruction.

When records have been transferred to the Provincial Archives of Alberta (e.g. in the case of Alberta Health and Wellness) or the archives of a custodian, the applicant should be advised that a request for the records should be made to the appropriate archives.

2.5.5 COPYING RETRIEVED RECORDS

Once the records have been located, either the program area in a larger custodian or the office of the Health Information Coordinator, as appropriate, prepares them for review and completes the request documentation.

This may involve copying and numbering all records pertinent to the request and preparing:

- a list of all records areas searched;
- a list of the records located in each records area, along with identifying data and parts of file lists, data dictionaries or other finding aids used in locating the records; and
- a log of staff time spent searching for and retrieving the records.

When there are a large number of records involved, lists of the records rather than copies of them may be more appropriate.

2.5.6 PRELIMINARY ASSESSMENT

Questions that the Health Information Coordinator should ask at this stage are:

- Have all relevant records been located and do they satisfy the request?
- Are there any records referenced in the request or in the located records that have not yet been located?
- Are any of the records subject to other legislation that prevails over the *Health Information Act*?
- Can the records, in whole or in part, be released immediately without line by line review?

- Where all or a portion of the request concerns records that were created by or are under the control of another custodian, should the applicant be advised of his or her right to make a separate request to that custodian?
- Should the search for records be widened?
- What is the extent and nature of consultation required with other program areas within the custodian? Responsibility for ensuring that these consultations occur should be clearly assigned.
- What is the extent and nature of external consultation required with other custodians or non-custodians? Responsibility for conducting these consultations should be clearly assigned.
- Will the time required to respond to the request likely exceed the 30-day time limit? Are there grounds for an extension of the time limit?
- Will fees be assessed for processing of the request?

Based upon this preliminary review, the Health Information Coordinator may, depending upon his or her level of responsibility, either recommend or undertake actions related to:

- the immediate release of all or some of the records;
- the extension of time limits; or
- the assessment of fees.

2.5.7 NOTICES

Various notices are required under the *Act*. Of particular importance are those provided:

- to inform an applicant of a fee estimate;
- to report to an applicant about the progress of a request (e.g. time limit extension); and
- to advise the applicant of the decision on the disclosure and provide information about access to the records if access is granted.

Section 103 provides that a notice or other document that is required by the *Act* to be given to a person be given:

- by sending it by prepaid mail to the last known address of the person;
- by handing it to the individual personally (i.e. personal service);
- by substitutional service, if that is authorized by the Commissioner; or
- by means of a machine or device that electronically transmits a copy of a document, picture or other printed materials by means of a telecommunications system.

The choice of how to give notice or send a document depends on the circumstances. Normal methods will be by mail and fax, since these are common, effective ways of communicating. There will be circumstances when other methods may have to be used. This may be the case when addresses are uncertain, or when there is a need to assure delivery to a specific person.

"Personal service" means a method of delivery where it can be shown that the person to be served actually received the document (e.g. using a process server).

"Substitutional service" usually takes the form of a notice presented in the media. This may be a general notice (appearing in newspapers and weekly journals) or a more specific notice published in certain trade magazines for a particular sector.

Custodians should assess the circumstances requiring the notice and choose the most economical and effective approach.

The **Model Letters B and C in Appendix 2** provide examples and options for the notices required under the legislation.

2.5.8 ESTIMATING, ASSESSING AND EXCUSING FEES

Section 7(3) states that the right of access to a record is subject to the payment of any fee required by the regulations. **Section 67(1)** gives custodians the power to charge the fees provided for in the regulations for services provided under **Part 2** of the *Act* **(Individual's Right to Access Individual's Health Information).**

The fees that may be charged relate to the steps that a custodian takes to produce a copy of the individual's own health information.

The Goods and Services Tax (GST) is not charged on fees for processing *Health Information Act* requests for the department, the regional health authorities, hospitals, nursing homes and provincial health boards. However, physicians and other small custodians will be required to charge GST on fees.

Under **section 10(1)** of the Health Information Regulation, a custodian may require an applicant who makes a request for access to a record containing health information to pay a basic fee of $25.00 for performing one or more of the following steps to produce a copy of the information:

- receiving and clarifying the request;
- obtaining consent if necessary;
- locating and retrieving the records;
- preparing the record for copying, including removing staples and paper clips;
- preparing a response letter;
- packaging copies for shipping or faxing, or both; postage and faxing costs; and
- photocopying a record.

Under the *FOIP Act*, the basic fee is called an initial fee but may only be charged for requests for general records, not personal information, under that *Act*. If the basic fee applies, a custodian will not start processing a request until the basic fee has been paid **(section 10(2)** of the Health Information Regulation).

In addition to the basic fee, a custodian may charge additional fees for producing a copy of a record, in accordance with the Fee Schedule. The fees set out in the Schedule are the maximum fees that can be charged to applicants **(section 1** of the Fee Schedule).

If the cost of photocopying a record, calculated at $0.25 per page, exceeds $5.00, the fees in the Schedule may be charged but only the amount that exceeds $5.00 may be charged **(section 2** of the Schedule).
The fees in the Schedule cover the costs of:

- copying records created in various media or formats;
- supervising an applicant's examination of original records;
- determining whether a record requires severing;
- reviewing and identifying the parts of the record to be severed;
- producing a record from an electronic record; and
- other direct costs such as charges to retrieve records or return records, or both, from another location, and courier charges, delivery charges, or both, to

send copies to an applicant other than by mail or fax.

Fee Estimates

Section 67(3) says that a custodian must give an applicant an estimate of the total fee for its services before providing the services.

Under **section 11(1)** of the Health Information Regulation, an estimate provided to an applicant must set out:

- the time and cost required to prepare the record for disclosure, including severing time and to retrieve records from another location;
- the cost of copying the record;
- the cost of computer time involved in locating and copying a record, or, if necessary, re-programming to create a new record;
- the cost of supervising an applicant who wishes to examine the original record, when applicable; and
- the cost of shipping the record or a copy of the record, other than by mail or fax.

The fee estimate is provided to the applicant as part of a notice that includes:

- a request that at least 50% of the estimate be paid in advance of the request being processed;
- a statement that the applicant has 20 days to inform the custodian that the estimate is accepted and to pay the deposit; and
- a statement that the applicant has the right to ask the custodian to excuse all or part of the fee and may request a review by the Commissioner if a request for fee waiver has not been granted.

Model Letter C in Appendix 2 may be used to provide this notice. The information in the notice gives the applicant the basis on which to accept the charges or take other action.

An applicant has up to 20 days to indicate if the fee estimate is accepted or to modify the request to change the amount of fees assessed **(section 11(2)** of the Health Information Regulation). The applicant may choose to modify the request so as to change the amount of fees assessed. In that case, a notice of a new fee estimate may need to be sent. If no response has been received after 30 days, the custodian may declare the request to be abandoned **(section 9). (See section 2.6 later in this Chapter).**

Fee estimates are not binding. However, a custodian should do its best to estimate what the fees will be. The custodian can revise its estimate in the course of processing the request, and may do so in cases where, for example, records are poorly organized. If the estimate is too high, a refund should be made to the applicant. If a fee estimate is too low, the custodian has the discretion to request additional fees from an applicant.

If the fees will be higher, this must be addressed with the applicant as soon as it becomes apparent and not be left to the end of the processing period.

Deposit and Payment of Fees

Section 12(1) of the Health Information Regulation says that processing of a request stops once a notice of estimate has been forwarded to an applicant and starts again immediately when the custodian receives an agreement to pay the fee and receives at least 50% of any estimated fee.

The custodian should wait until:

- a letter from the applicant agreeing to the charges and attaching payment of the deposit is received in the authorized office of the custodian;
- written notification from the applicant modifying the request, and establishing a new basis for assessment of fees, is received in the authorized office of the custodian;
- the custodian agrees to a request for a fee waiver; or
- the Commissioner carries out a review and decides whether the fees are appropriate, or whether the custodian has appropriately exercised discretion regarding a request for excuse of payment of fees, as applicable.

The balance of any fee owing is payable at the time the information is delivered to the applicant **(section 12(2)** of the Health Information Regulation**).**
If the amount paid is higher than the actual fees required to be paid, the balance paid will be refunded.

The applicant should not be provided with access to a record until all fees owing for the processing of the request have been paid **(section 7(3)** of the *Act).*

Custodians, other than the department, should arrange for fees paid to be handled in the same way as other revenue. The department must process fees in accordance with directions from Alberta Treasury.

Excusing the Payment of Fees

Section 67(4) allows a custodian to excuse an applicant from paying all or part of a fee if, in the opinion of the custodian, the applicant cannot afford the fee or in any other circumstances provided for in the regulations.

Section 13 of the Health Information Regulation says that the "other circumstances" would depend upon the opinion of the custodian as to whether it would be fair to excuse payment of all or a part of a fee.

If the custodian refuses an applicant's request to excuse the payment of all or part of a fee, the custodian must notify the applicant that the applicant may ask for a review by the Commissioner **(section 67(5)).**

Normally, an applicant will take the initiative in requesting that fees be excused, usually at the time of submitting the request. A custodian must consider the request for such an excuse from an applicant at the time it is made. If a request for excusing the payment of fees is part of the *Health Information Act* request, the custodian will consider this when it is preparing a fee estimate and decide whether an excuse of payment is merited.

The custodian does not need to excuse the payment of all fees if it decides to grant such a request. It can consider reducing the fee by a part of its total or not charging for certain services.

Reasons for Excusing the Payment of Fees

1. Applicant Cannot Afford to Pay

Applicants who are indigent or living on social benefits may require access to their health information. Normally, applicants will state in a request why they are seeking to excuse the payment of fees. If they do not or if more information is required, the Health Information Coordinator or whomever is dealing with the applicant should phone the applicant and seek the information needed to make a decision.

Applicants should not have to undergo a wealth or means test to qualify for this type of payment excuse but basic information on income and situation should be sought to satisfy the custodian that an applicant may fall into this category. For instance, applicants may be asked to show evidence that they would suffer hardship if they were obliged to pay the required fee, including general information about their sources of income.

2. It is Fair to Excuse Payment

This provision covers situations where a custodian is of the view that reducing or excusing fees would be fair or appropriate under the circumstances of that particular applicant and that particular request.

An example of this might be where an individual can show that access to his or her own health information is vital to the exercise of his or her rights.

2.5.9 CONSULTING WITH OTHERS

In some cases, the records requested may include information that could be subject to a discretionary exception under **section 11(1)** and another custodian may need to be consulted to determine whether portions of the record(s) should be severed under an exception. For example, a hospital may need to consult with an individual's private physician to determine if disclosure of the records could reasonably be expected to result in harm to the applicant, to threaten the health or safety of another individual or to pose a threat to public safety **(section 11(1)(a))**.

On the other hand, if a health record includes referral letters containing health information from other custodians or health information provided by another physician acting in a consultant capacity, consultation with the other physician before disclosing the records, subject to any applicable exceptions, would not normally be required. The existence of those records on the applicant's file may lead the applicant to make a request for access to their own health information that may be in the custody of that other custodian.

2.5.10 REVIEWING RECORDS

Once the preliminary assessment has been completed, the various administrative matters have been sorted out and any necessary consultations are under way, someone will need to review the record(s) line by line. This could be done by a knowledgeable officer from the area responsible for the requested records; someone in the office of the Health Information Coordinator; or in small offices or an office of a single custodian, a person knowledgeable about the records and knowledgeable about the exceptions under the *Act*.

A line by line review is essential to comply with the principle of severability set out in **section 7(2).** This provision grants an applicant a right of access to any record containing their own health information from which excepted information can be reasonably severed.

Chapter 3 of this Publication deals with the guidelines for the application of the exceptions to the right of access. A person knowledgeable about the records can offer their perspective on any harm that may result from release of particular information and can identify factors to be taken into consideration when exercising discretion to release or refuse access to the information. During the line by line review, the office of the Health Information Coordinator (for larger custodians) may identify additional requirements with respect to consultations.

Documentation

During the line by line review, the reviewer should document exceptions to be invoked (based upon **section 11),** actions to be taken, reasons for each decision, and recommendations for responding to the request.

An **Access Request Review Form** is provided in **Appendix 1 of this Publication** and may be adapted for internal use. This form provides a detailed record of the results of the review and recommendations on the application of exceptions.

Thorough documentation at this stage ensures that the custodian has the information required to assess recommendations and to make final decisions relatively quickly. It minimizes duplication of effort and ensures that the custodian is in a position to explain decisions both to the applicant and to the Office of the Information and Privacy Commissioner, if there is a request for a review.

Reviewer's Recommendations

The reviewer should prepare a summary of recommendations that identifies:

- information recommended for release;
- specific records or parts of records excluded from the scope of the *Act* or which may be deemed to be included in a request for access to information under the *FOIP Act;*
- specific records or parts of records to which mandatory or discretionary exceptions to disclosure apply, with the reviewer's recommendations and reasons with respect to the discretionary exceptions **(see Chapter 3 of this Publication for guidance on the exercise of discretion**); and
- other general factors that may be pertinent in reaching a decision on a response to the request.

For larger custodians, these recommendations can form the basis for a discussion on the contents of a response between the office of the Health Information Coordinator and the area responsible for the records, or between the Coordinator and the official who makes release or refusal decisions.

For smaller custodians, the discussion might occur between a physician or pharmacist and the staff member who reviewed the records. For single custodians, the above recommendations could act as a checklist for decision-making.

At this stage, any legal advice needed to resolve issues arising from the request should be sought. Any interpretive or policy issues which need to be raised should be identified and consultation undertaken.

For larger custodians, a designated Health Information Coordinator or other official designated to make decisions regarding access requests should prepare a final report containing:

- a log of staff time spent copying the records and for locating, retrieving and reviewing records;

- a summary of file systems, offices and records storage facilities searched;
- copies of records relevant to the request (where this is possible and appropriate given the volume of records or the fact that the applicant wishes to view the original records);
- documentation of the line by line review, identifying the specific information that is proposed to be excepted from access;
- a summary of results of consultations with other custodians (where that has occurred); and
- a written summary of recommendations for release or refusal, including any background information to explain decisions.

The **Access Request Recommendation Form in Appendix 1 of this Publication** can serve as the authority to produce the response to the applicant and should be signed by the official who has been designated as responsible for making decisions about access on behalf of the custodian. For smaller, simpler requests, or where a request is made to a single custodian, a written memo documenting the information above for the final report, approved by the individual designated as the responsible person to approve responses to applicants, would be sufficient for this purpose.

Responsive Information

Records that have been retrieved in an initial search may include information that is not responsive to the request. Careful examination of the request is required to ensure that the reply is complete but also that information that does not respond to the request is removed.

The fact that an applicant already has or knows the substance of the information or has knowledge of the contents of the records, does not mean that the record can be considered non-responsive. The obligation of the custodian is to address the applicant's entire request **(see IPC Order 98-005).** However, a custodian and an applicant may agree not to make copies of certain records (that an applicant may already have) in order to save costs.

Removal of non-responsive information must occur before severing takes place in accordance with the exceptions in the *Act*. A custodian may treat portions of a record as non-responsive if they are clearly separate and distinct and entirely unrelated to the access request **(see IPC Order 97-020)**.

2.5.11 SEVERING INFORMATION

Records may contain both information that can be released and other information that should be excepted from disclosure. When information that falls within an exception can reasonably be severed from a record, an applicant has a right of access to the remainder of the record **(section 7(2)).**

When a discretionary exception applies, a custodian must use discretion not only in applying the exception, but also in determining how much of the information is severed. This is the reason for doing a line by line review of a record. The object of severing is the use of discretion to release as much information as possible, without causing the harm contemplated by the exception.

Scope

Severing applies to all records regardless of format or previous actions taken. The fact that an applicant may have already obtained copies of some of the records in other ways does not preclude severing to respond to a request **(see IPC Order 98-016)**.

When severing is required for information stored on specialized media, technical expertise should be sought as to the best way to excise information while recording that severing has been done and for what reason. In some cases, a record cannot be severed. The custodian must then refuse access to the whole record and must be prepared to demonstrate to the Information and Privacy Commissioner the technical reasons underlying the inability to sever. Examples include the health information of two or more individuals so intertwined in a record that severing would be extremely difficult and time-consuming, or when, after severing, the severed record would make no sense **(see IPC Order 96-019)**.

Procedures

During the line by line review of records pertinent to a request, the reviewer should mark up copies of paper-based records and keep notes about information in other media that may qualify for an exception. The review and severing of records may require a significant amount of time. The procedure should ensure that all records responsive to the request are reviewed.

The objective in severing is to remove only the information that falls within an exception. The *Act* requires that all health information contained in a record that is responsive to the request and that will be intelligible to the applicant after severing, be disclosed.

The severing process is governed by reasonableness, and the custodian exercises discretion in determining whether discrete portions of information contribute to the overall understanding of the subject matter at issue.

***BEST PRACTICE:** Where affiliates are drafting health records that contain information that could be subject to an exception (e.g. recommendations for advice, or another individual's health information), they should be encouraged to draft the record so that such information is put in a separate section of the record. This will make the severing process more efficient.*

Part of the final decision as to what information will be released and what information will be refused is also a decision on the extent to which the severing process will be applied. Once that decision is made, the Health Information Coordinator, or other individual authorized to do the severing, can use several methods of severing:

- use of non-permanent white tape over the excepted portion of a copy of the record and recopying to obtain the record to be released;
- use of liquid eraser over the excepted portion of a copy of the record and recopying to obtain the record to be released; or
- use of a photocopying machine with editing features suitable for severing.

Whatever method of severing is selected, the Coordinator or person with this designated responsibility must ensure that none of the excepted information remains visible. For this reason, the use of markers is not recommended.

Indication of Severing

A custodian must indicate the section number (and subsection, where applicable) of any exception used to sever information, either in the space left after the severing or in the margin closest to the severed information. If an entire page is removed, the number of pages severed must be indicated, along with a reference to the applicable exception(s) used to sever the information.

In cases where a single page or a continuous sequence of pages has been totally severed, the exception(s) applied and the pages to which they applied should be listed in the response letter or collated on a single page. It is not necessary or helpful to provide applicants with multiple blank pages.

In some cases, especially with mandatory exceptions, placing the relevant section in the space of the severed information may itself reveal or imply information that could cause harm. In these circumstances, it is permissible for the custodian to omit section numbers on the severed pages and list the relevant sections supporting severance in the letter of notification.

Indicating the section numbers used to sever information from records helps an applicant understand why part of the information requested has been refused and permits an independent review of the decisions made by the custodian. The applicable sections of the *Act* could be included in the response to the applicant for greater clarity.
See IPC Practice Note No. 2, Informing the Applicant of Grounds for Refusal.

2.5.12 DOCUMENTING AND TRACKING REQUESTS

Custodians should maintain documentation systems to record all deliberations and decisions regarding the processing of requests and to help ensure that the request process meets the requirements set out in the *Act*.

The documentation may become a critical part of the evidence required during a review by the Information and Privacy Commissioner. It can also be of assistance in processing subsequent similar requests **(see IPC Order 99-011).**

The 30 day time period for responding to requests starts on the day after receipt of a request in the office of the custodian designated to receive such request. In a large or decentralized custodian, this would normally be the office of the Health Information Coordinator. A request may be delivered to any office of a custodian during normal business hours, but the time limit for responding does not start until the request is received in an office authorized to receive requests.

Custodians need to have a reasonable system in place to ensure that requests are forwarded immediately to the office(s) designated to receive and begin processing them.

Reasonable steps might include special forwarding instructions to staff in mail rooms within the custodian and to staff who open the mail, as well as use of a color-coded transmittal file to indicate the priority and important nature of the request. Staff should be made aware of the urgent nature of requests under the *Health Information Act* and the need to forward them immediately to the Health Information Coordinator or person designated as responsible for responding to requests.

Once the request is received in the authorized office, it should be date-stamped.

Custodians may establish an automated or manual tracking system depending upon the volume of work generated by requests under the *Act*. Tracking systems help ensure that the time periods under the *Act* are complied with and keep track of progress in responding to a request. Automated systems are not normally needed unless a custodian receives more than 50 requests annually or the custodian is decentralized and there is a need to coordinate responses. Database management software, such as Microsoft Access, could be used to develop an automated tracking system for requests.

2.5.13 MAINTAINING COPIES OF REQUESTS AND RECORDS

***BEST PRACTICE:** Custodians should keep a file for each request processed under the Act. This file should include:*

- *all internal and external correspondence, including a copy of the original request from the applicant, any notices sent to the applicant and any other correspondence from the applicant;*
- *an unmarked copy of the records retrieved and reviewed in response to a request;*
- *a copy of the documents released to the applicant, either severed or complete; and*
- *any other information documenting the request management process.*

This practice helps support the custodian in any review by the Information and Privacy Commissioner, and in making decisions regarding requests for the same or similar records in the future. However, unless the new request is made shortly after the original, there is still a need to review the records again **(see IPC Order 99-021).**

The passage of time and any changes in the context surrounding the records may result in more information being released. Each request needs to be processed as a separate request and decisions need to be made in relation to the particular circumstances that apply at the time of the request.

This does not mean that every request is unique. There may be similar types of requests that lend themselves to categorization and simple release mechanisms. It may be possible to create easily severed documentation that is then released routinely to the individual it is about.

2.5.14 CLOSURE AND RETENTION OF REQUEST FILES

It is a good practice to keep a request file active for at least 60 days after responding to a request in order to allow time for a request for a review by the Commissioner. If a review is requested, the file will be reopened and remain open until the review process is complete.

Once the file is closed, either because the custodian has responded to the request, a review has been completed, or a request has been declared to be abandoned, the custodian must retain the request file for the period of time authorized by its retention and disposition schedule. Custodians must not transfer, store or destroy request records except in accordance with such authorization.

2.6 ABANDONMENT OF REQUESTS

Sometimes applicants will indicate in writing or by telephone an intention not to proceed with a request. This may be because they have found that the information is available to them outside the access request process under the *Act* or because they no longer need the information.

However, an applicant may simply cease to respond during the processing of a request. When this situation occurs, **section 9** sets out the provisions for declaring a request to be abandoned. The custodian must have contacted the applicant in writing, and either sought further information necessary to process the request, or requested payment of or agreement to pay a fee.

If the applicant does not respond within 30 days of being contacted, the custodian may advise the applicant, in writing, that the request has been declared abandoned as of a specific date. This notice must state that the applicant can ask for a review of the decision by the Commissioner.

In some cases, an applicant abandons a request after processing is completed. If the custodian:

- has responded to the applicant's request, stating where, when and how access will be given;
- has requested that the applicant contact the custodian about viewing the records; and
- the applicant does not respond within 30 days,

the custodian may advise the applicant that the request has been declared abandoned.

The file should be kept active for a further 60 days in order to allow time for the applicant to request a review by the Commissioner.

Model Letter D in Appendix 2 deals with this type of situation.

THINGS TO REMEMBER

ACCESS TO AN INDIVIDUAL'S OWN HEALTH INFORMATION

- An individual has a right of access to any record containing health information about the individual that is in the custody **or** under the control of a custodian, subject to the payment of any required fees and subject to the custodian being authorized or required to refuse access under *section 11* of the *Act.*
- **"Custody"** means having possession of the health record or information and having the right to deal with the record it.
- **"Control"** means having the authority to manage the health record or information by such things as restricting, regulating and administering its use, disclosure or disposition.
- If a custodian has another procedure for an individual to access his/her own health information, the individual may choose to use the existing procedure.
- The access request process under *Part 2* of the *Act* may be used by an individual who has not been able to use an access process outside the *Act* or who has not been satisfied with the amount or kind of information received through another process.
- The *Act* does not prevent or limit the use of legal processes to gather information about a party in a legal action and the *Act* does not override the power of a court to compel a witness to testify or a custodian to produce documents.
- A request for access to an individual's own health information may be written or non-written depending upon the policy of the custodian and may use the Request to Access Information Form (in Appendix 1 of the Manual).
- An individual's right of access may be exercised by an authorized representative, such as a parent, guardian, executor, etc., with documented authority (section 104(1)(c) to (h). An individual may give written authorization to another person to act on his/her behalf (under section 104(1)(i)) or by using an Authorization of Representative Form (sample in Appendix 1 of the Manual).
- A custodian must ensure that the identity of the applicant or the applicant's representative is authentic.

- If a custodian is subject to both the *Health Information Act* and the *FOIP Act* and receives a request for access to an individual's personal information, the rules under the *Health Information Act* would apply to accessing the individual's own health information and the rules under the *FOIP Act* would apply to accessing the individual's other personal information.
- A custodian may charge an applicant the fees in the Schedule under the Health Information Regulation but may also excuse the applicant from paying all or part of the fees. The fees in the Schedule are intended to be maximums. Custodians may charge applicants less than the amounts in the Schedule.
- A request for access to an individual's own health information must be completed within 30 calendar days unless the time limit has been extended in accordance with the *Act*.

For help in processing a request, refer to the Model *Health Information Act* Access Request Chart for a list of key tasks and timelines; to the Model Letters for responding to an applicant (in Appendix 2 of the Manual); and to the Forms for Access Request Review and Access Request Recommendation (in Appendix 1 of the Manual).

Calendar Days	Responsible Person/Area	Key Tasks	Manual References
Day 1	HIA Coordinator or Responsible Affiliate (person responsible for Coordinating Request Process)	Review request.	
		Confirm that it is an access request under Part 2 of the Act.	2.4.1
		If the information can be released through a more routine process, advise the applicant of that option.	
		Confirm that the request is for records covered by the Act.	
		Register and Log receipt of the request.	2.5.1
		If processing cannot begin immediately, contact the applicant directly to define or clarify the request.	2.5.2
		Acknowledge receipt of the request.	2.5.3
		Collect basic fee if applicable.	2.4.5
		Create request file.	2.5.1
		If part of the request is deemed to be a request under the FOIP Act, provide an explanation of how the FOIP request will be dealt with.	2.4.6
		If another custodian may have some or all of the records requested, advise applicant that they may make a separate request to that custodian.	2.4.1
Day 2-6	HIA Coordinator or Responsible Affiliate	Request records from the area(s)/affiliate(s) that most likely have the responsive records (if applicable).	
	Responsible area/affiliates	Locate and retrieve the records.	2.5.4
		Report the results of the record search to the HIA Coordinator or person designated as responsible.	2.5.4
Day 6	HIA Coordinator	Prepare records for review and complete the request documentation.	2.5.5
		List areas searched.	
		List records located.	
		Log staff time spent searching and retrieving records.	
		Copy and number retrieved records (to make a working copy).	2.5.5
		Conduct preliminary assessment.	2.5.6
		Conduct additional fee estimate.	2.5.8

Calendar Days	Responsible Person/Area	Key Tasks	Manual References
Day 6 Cont'd	HIA Coordinator	Requests for large amounts of information can result in significant fees being assessed. If required, try to narrow the request while still meeting the applicant's needs. If the request has been changed, document the change and send a notice to the applicant.	2.5.7
Clock Stops	HIA Coordinator	Collect 50% of the estimated fee. Suspend processing until 50% of the fee is received.	2.5.8
Day 7-10	HIA Coordinator	Initiate consultations with other area(s)/affiliate(s) and others as required.	2.5.9
Day 11	Coordinator	Extend time limit for response? Notify applicant if time limit is extended.	2.5.7, 2.4.3, 2.4.4
Day 12-22	Coordinator	Knowledgeable HIA/responsible staff to complete detailed line by line review of the records and apply exceptions. Document exceptions. Prepare recommendations and get program area approval (if required).	2.5.10 2.5.10 2.5.10
Day 23-28	HIA Coordinator	Final analysis of reviews and recommendations. Prepare final recommendations for the official who makes decisions on the access requests.	2.5.10
Day 29	HIA Coordinator	Sever records and indicate the section number used to severe the information. Prepare records for applicant.	2.5.11
Day 30	HIA Coordinator	Send response letter to applicant (either regarding the balance of fees owing or enclosing copies of the records if fees are paid). Maintain copies of request records.	2.4.7 2.4.13
Clock Stops	HIA Coordinator	Collect balance of fees owing if applicable. No further processing until fee balance received.	2.4.5, 2.5.8
Day 90	HIA Coordinator	Keep files active for 60 days to allow time for a request for review by the IPC. Then close the file and retain the record according to authorized retention and disposition schedules.	2.5.14 2.5.14

CHAPTER THREE

EXCEPTIONS TO THE RIGHT OF ACCESS TO AN INDIVIDUAL'S OWN HEALTH INFORMATION

3.1 OVERVIEW OF CHAPTER THREE

This Chapter will cover:

- the meaning of the right to refuse an individual's request to access their own health information;
- the meaning of "harm";
- how a custodian "exercises its discretion" in applying the exceptions to disclosure;
- the discretionary exceptions; and
- the mandatory exceptions.

Note that the references to Orders and Practice Notes of the Information and Privacy Commissioner used in this Chapter relate to the *FOIP Act*, not to the *Health Information Act* and are only used to illustrate or clarify a point. They do not create a precedent and are not a definitive interpretation of the *Health Information Act* by the Commissioner.

3.1.1 RIGHT OF ACCESS SUBJECT TO SPECIFIC AND LIMITED EXCEPTIONS

Section 2(d) provides individuals with a right of access to health information about themselves, subject to limited and specific exceptions as set out in the *Act*. These exceptions are set out in **section 11.**

Although custodians are authorized and in some cases, required to refuse access to a record or to a portion of a record, a basic principle of the *Act* is to give individuals access to their own health information. Any exceptions to this right of access should be applied in a limited and specific way to provide as much access to their information as possible. Refusal to disclose all or part of a record will occur only where there is a specified exception to the disclosure that is supported by a provision of the *Act*.

Each record must be carefully reviewed to determine if there is harm in releasing certain information in the record; whether this harm qualifies for an exception under the *Act;* or whether disclosure would reveal a certain class of information that falls within an exception.

Custodians should interpret the exceptions narrowly. This means that there must be a reasonable expectation that an exception applies, and only the specific information that is subject to the exception will be withheld.

In some cases more than one exception may apply to all or part of a record. A custodian should take into account all relevant factors when considering an exception to an applicant's right of access.

Refusals of access to an individual's own health information are likely to form the basis of the majority of requests for reviews to the Information and Privacy Commissioner under **section 73.** Custodians should be prepared to document and defend their decision not to disclose particular information.

Discretionary Exceptions

The exceptions in **section 11(1)(a) – (e)** start with the phrase "a custodian may refuse to disclose health information". They permit a custodian to disclose a record despite the existence of the exception. There are five discretionary exceptions.

Discretionary exceptions require two decisions by a custodian:

- a determination as to whether a record comes within the description of records potentially subject to being withheld from disclosure; and
- the exercise of discretion by a custodian must be made as to whether the record should still be disclosed even though it might qualify for the exception.

See section 3.3 of this Chapter for a discussion of the Discretionary Exceptions.

Mandatory Exceptions

The exceptions in **sections 11(2)(a) –(d)** start with the phrase "a custodian must refuse to disclose". If information falls within a mandatory exception, a custodian must refuse to disclose all or part of the record as required. There are four mandatory exceptions.

See section 3.4 of this Chapter for a discussion of the Mandatory Exceptions.

3.1.2 MEANING OF HARM

"Harm" means loss or detriment. Each exception is designed to prevent the occurrence of particular "harms".

Many discretionary exceptions are based on applying a "harms test". This means that access to all or part of a record may be refused if disclosure could reasonably be expected to harm a particular public or private interest.

Three general factors should be taken into account in making a judgment as to harm.

- **The harm must be specific:** To qualify, it must be possible to identify the detrimental effect with the actual party whom or the actual interest which will suffer harm. The loss or injury cannot be a vague, general harm.

- **The harm must be current:** To qualify, it must be possible to identify the detrimental effect at the time the exception is claimed or in the foreseeable future. Records which have been protected from disclosure in the past should be reassessed when a new request is received to ensure that the harm is still a factor.

- **The harm must be probable:** To qualify, there must be a reasonable likelihood of the harm occurring.

  Some of the factors that will impact a potential harm:
  - the timing of the request;
  - the context of the request;
  - the value of the information to the custodian;
  - the public availability of the information; and
  - the confidentiality of the information.

(See IPC Practice Note No. 1 – applying "Harms" Tests, May 1996).

3.1.3 REVEALING A CLASS OF RECORDS

A few discretionary exceptions are based on preventing a class of record from being revealed rather than on preventing the occurrence of a particular harm. For example, a custodian may refuse to disclose all or part of a record containing advice, proposals, recommendations, analyses or policy options developed by or for a member of the Executive Council. In such cases, there is no need to address the harm that the disclosure may entail.

3.1.4 EXERCISING DISCRETION

The exercise of discretion requires that the custodian determine whether harm is likely to result from the release of information that falls within the exception or, if the exception does not have a harms test, whether the interest outlined in the exception should be protected. If no harm is apparent or the particular interest is not adversely affected, the custodian should release the information.

The custodian must take into account all the relevant circumstances of the request and any advice obtained either from officials within the custodian or from other custodians or other concerned parties in determining whether or not information that qualifies for a discretionary exception can be disclosed.

The exercise of discretion should be:

- reasonable;
- adapted to the circumstances; and
- non-discriminatory.

In a review situation, the Information and Privacy Commissioner will decide whether an exception applies in a particular circumstance. However, if a discretionary exception has been properly applied, the Commissioner is not likely to overrule the custodian's decision. The Commissioner can, however, order that discretion be exercised properly, where it appears that this responsibility is being disregarded or done without due care and diligence.

A custodian must not replace the exercise of discretion with a blanket policy that information will not be released if it falls within an exception. However, guidelines can be developed to help guide the exercise of discretion, provided they are not interpreted as binding rules.

Some factors that should be taken into account when exercising discretion include:

- the general purposes of the legislation;
- the wording of the discretionary exception and the interests which the exception attempts to balance;
- whether the applicant's request could be satisfied by severing the record and by providing the applicant with as much information as is reasonably practicable;
- the historical practice of the organization with respect to the release of similar types of records;
- the age of the record; and
- whether previous Commissioner's orders have ruled that similar types of records or information should be disclosed.

(See IPC Order 96-017)

3.1.5 APPLICATION OF EXCEPTIONS AND RESPONSE TO APPLICANT

The basic steps in applying exceptions are:

Step 1: Preliminary Examination
Review the record(s) to determine which exceptions may apply and to gauge the complexity of the request.

Step 2: Detailed Review
Review the record(s) line by line to thoroughly consider the nature and extent of the exceptions involved, including mandatory exceptions where the custodian has no discretion to disclose information and identification of information where no exception applies.

Step 3: Exercise of Discretion
Where discretion is permitted, decide whether all or part of the information subject to the exception will be released or refused.

Step 4: Severing
Sever the part of the record(s) to which the custodian has decided that it is necessary to refuse access. This will leave the record with blank spaces.

Step 5: Response to Applicant
Prepare a response to the applicant following the guidelines provided in **Chapter 2 of this publication.**

Following the explanation for each exception in section 11, a flowchart diagram outlines the steps for applying the exception. A diamond in the flowchart represents the questions that the custodian should be considering in each step. A circle represents a decision that the exception being considered does not apply to the information or record under review. A square represents a decision to apply the exception or disclose the information or record to the applicant.

3.2 RELATIONSHIP TO OTHER ACTS

Inconsistency or Conflict with Another Enactment

Section 4 states that if a provision of the *Health Information Act* is inconsistent or in conflict with a provision of another Act or regulation, the provisions of the *Health Information Act* prevail unless

- another act, or
- a regulation under the *Health Information Act* expressly provides that the other Act or regulation, or a provision of it, prevails over the *Health Information Act.*

Some acts have specific provisions that will prevail over the *Health Information Act* once it is in force (e.g. Part 1.1 of the *Cancer Programs Act;* and section 22(3) of the *Fatality Inquiries Act).*

When considering records that might be excepted under **section 4,** a custodian has to be sure that the record(s) being reviewed have a direct relationship to the provision that prevails **(see IPC Order 98-007).**

If the Commissioner finds that a provision of the *Health Information Act* is inconsistent or in conflict with another enactment, and the other enactment is one that prevails, he has no jurisdiction over the information with respect to that provision **(see IPC Order 99-034).**

(See the discussion of Inconsistency or Conflict with Another Enactment under section 1.6 in Chapter 1 of this Publication)

Deemed Requests Under the *FOIP Act*

For a discussion of the relationship between requests under the *Health Information Act* and requests under the *FOIP Act*, **see section 2.4.6 of Chapter 2 of this Publication (section 16 of the *Health Information Act*).**

Copyright Act

Section 32.1 of the *Copyright Act (Canada)* states that disclosure of a record pursuant to the *Access to Information Act (Canada)*, or disclosure pursuant to any like act of the legislature of a province, does not constitute an infringement of copyright.

Although this is unlikely to occur, custodians would not infringe copyright by disclosing copyrighted material in response to a request for health information under the *Health Information Act*.

3.3 DISCRETIONARY EXCEPTIONS

3.3.1 DISCLOSURE EXPECTED TO HARM OR THREATEN THE APPLICANT'S OR ANOTHER INDIVIDUAL'S MENTAL OR PHYSICAL HEALTH OR SAFETY OR POSE A THREAT TO PUBLIC SAFETY

Section 11(1)(a) provides a custodian with discretion to refuse to disclose health information to an applicant if the disclosure could reasonably be expected to:

- result in immediate and grave harm to the applicant's mental or physical health or safety;
- threaten the mental or physical health or safety of another individual; or
- pose a threat to public safety.

"Immediate and grave harm" means something that would cause very serious physical or mental trauma to an applicant or would pose considerable danger to the safety of an applicant. The harm would also have to reasonably be expected to occur without delay or within a very short time after the information is disclosed.

An example of where this exception may be relevant would be an individual with a long history of mental instability who might suffer serious mental and physical trauma if a certain diagnosis were made available to him or her without the benefit of medical or mental health intervention.

"Threaten" means to expose to risk or harm.

"Safety" means the relative freedom from danger or risks.

"Mental health" refers to the functioning of a person's mind in a normal state.

"Physical health" refers to the well-being of an individual's physical body.

The following example may help to illustrate the concept of an individual's mental or physical health being threatened. If there is information in an applicant's health record (e.g. informant information) and there is a good possibility that disclosure of the information to the applicant could cause danger or harm to the informant, the custodian may wish to apply this exception.

In determining whether such a threat exists, a duly qualified person (physician, chartered psychologist, psychiatrist or other appropriate expert) (who might also be the custodian of the information) could exercise his or her judgment about the potential for harm to occur.

In the case of a request for records made to a custodian with many affiliates and facilities, it could consult with its own health professional staff or a duly qualified health professional external to the custodian to determine whether there was a threat to the mental or physical health or safety of another individual.

Individual safety could be threatened if, for example, registration information was released to an applicant, allowing him or her to locate an individual that he or she had previously threatened to injure or kill.

"Pose a threat to public safety" means that the disclosure of information could present a risk that the functioning of organizations and structures that ensure the safety and well-being of the public at large would be hampered or blocked.

An example of this would be where a custodian feels that an applicant wants to release details of his own health information to the public for the purpose of creating widespread panic or stress. The result of this could be patients overloading emergency rooms, physician's offices or laboratories, which could delay the treatment of those in genuine need of care.

BEST PRACTICE: *If a custodian feels that the disclosure of certain information could result in the harms specified in this exception, the custodian should make an effort to provide the applicant with as much health information as possible by using an appropriate health services provider to explain the meaning of the information to the individual or to put it into context with the individual's other health information.*

Application of Exception

Figure 1 contains a flowchart setting out the application of **section 11(1)(a)**.

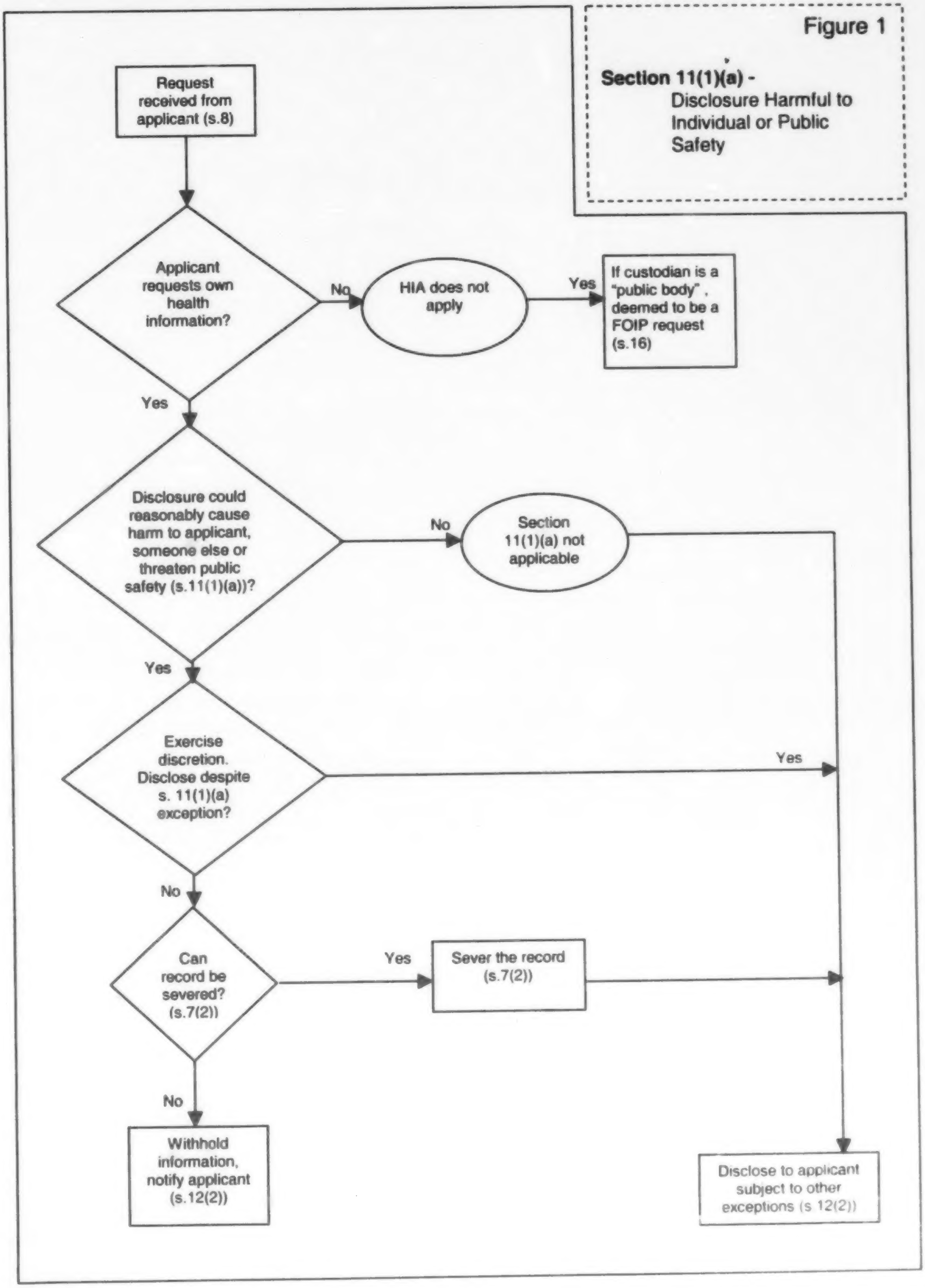


Figure 1

Section 11(1)(a) - Disclosure Harmful to Individual or Public Safety

Request received from applicant (s.8)
Applicant requests own health information?
No
HIA does not apply
Yes
If custodian is a "public body", deemed to be a FOIP request (s.16)
Yes
Disclosure could reasonably cause harm to applicant, someone else or threaten public safety (s.11(1)(a))?
No
Section 11(1)(a) not applicable
Yes
Exercise discretion. Disclose despite s. 11(1)(a) exception?
Yes
No
Can record be severed? (s.7(2))
Yes
Sever the record (s.7(2))
No
Withhold information, notify applicant (s.12(2))
Disclose to applicant subject to other exceptions (s 12(2))

3.3.2 DISCLOSURE LEADING TO IDENTIFICATION OF A CONFIDENTIAL SOURCE OF HEALTH INFORMATION

Under **section 11(1)(b)** a custodian may refuse to disclose health information (e.g. registration information) that could reasonably lead to the identification of a person who provided health information to the custodian explicitly or implicitly in confidence. To fit within the exception, the person who provided the health information must also have done so in circumstances where it would be appropriate that the name of the person be kept confidential.

The exception does not require a custodian to demonstrate that harm could come to the source but must make a determination, based on the relevant circumstances, that it is appropriate to protect the identity of the source.

"Identity" includes the name and any identifying characteristics, symbols and numbers relating to the source.

A **"confidential source"** is someone who supplies health information, as defined in the *Act,* to a custodian on the assurance that his or her identity will remain secret. Affiliates cannot be **"sources"** because they are employees or contractors of a custodian and are supplying information as part of their job **(see IPC Order 99-010).**

"Explicitly" means that there is written or other documentary evidence that indicates that the information was supplied on the understanding that it would be kept confidential.

"Implicitly" means that both parties understand the confidentiality even though there may be no actual statement, written agreement or other physical evidence of the understanding. All relevant facts and circumstances need to be examined to determine whether there is an understanding of confidentiality.

"In confidence" usually describes a situation of mutual trust in which private matters are related or reported.

Some factors that may be considered when determining whether information was supplied explicitly or implicitly in confidence are:

- whether there is documentary evidence indicating that confidentiality exists;
- the representations of the source as to his/her understanding of confidentiality;
- past practice of the custodian, particularly whether similar information has normally been kept confidential in the past;
- the confidentiality with which it is maintained by the source;
- whether the information was supplied voluntarily; at the request of the custodian; or as required by law, and the consequences for the source if it does not supply the information; and
- actions taken by, or conduct of, the custodian and the source, which may indicate an understanding of confidentiality.

(Taken from IPC Order 97-013 which, in the context of section 15(1)(b) of the *FOIP Act,* interprets what supplied "in confidence" means.)

It is not sufficient to accept a stamp marked "Confidential" on a document from a source or a statement by the source that information was supplied in confidence. There must also be supporting evidence to prove that the information has been treated consistently in a confidential manner.

IPC Order 96-020 discusses the confidentiality of informant information in the context of a report made to the Health Facilities Review Committee.

Where a custodian can demonstrate that the source is confidential and is supplying health information, it then determines whether the information requested by the applicant could permit the applicant or anyone else to identify the source. Since it may be difficult to determine whether information can be linked to provide identification, caution should be exercised in releasing any information connected to a confidential source.

In determining whether it would be **"appropriate in the circumstances"** not to disclose the name of the source, a custodian would have to look at all the circumstances in which the health information was provided. This would include weighing any policy reasons for maintaining confidentiality and deciding whether the public interest, in this instance, favored disclosure or non-disclosure.

Application of Exception

Figure 2 contains a flowchart setting out the application of **section 11(1)(b).**

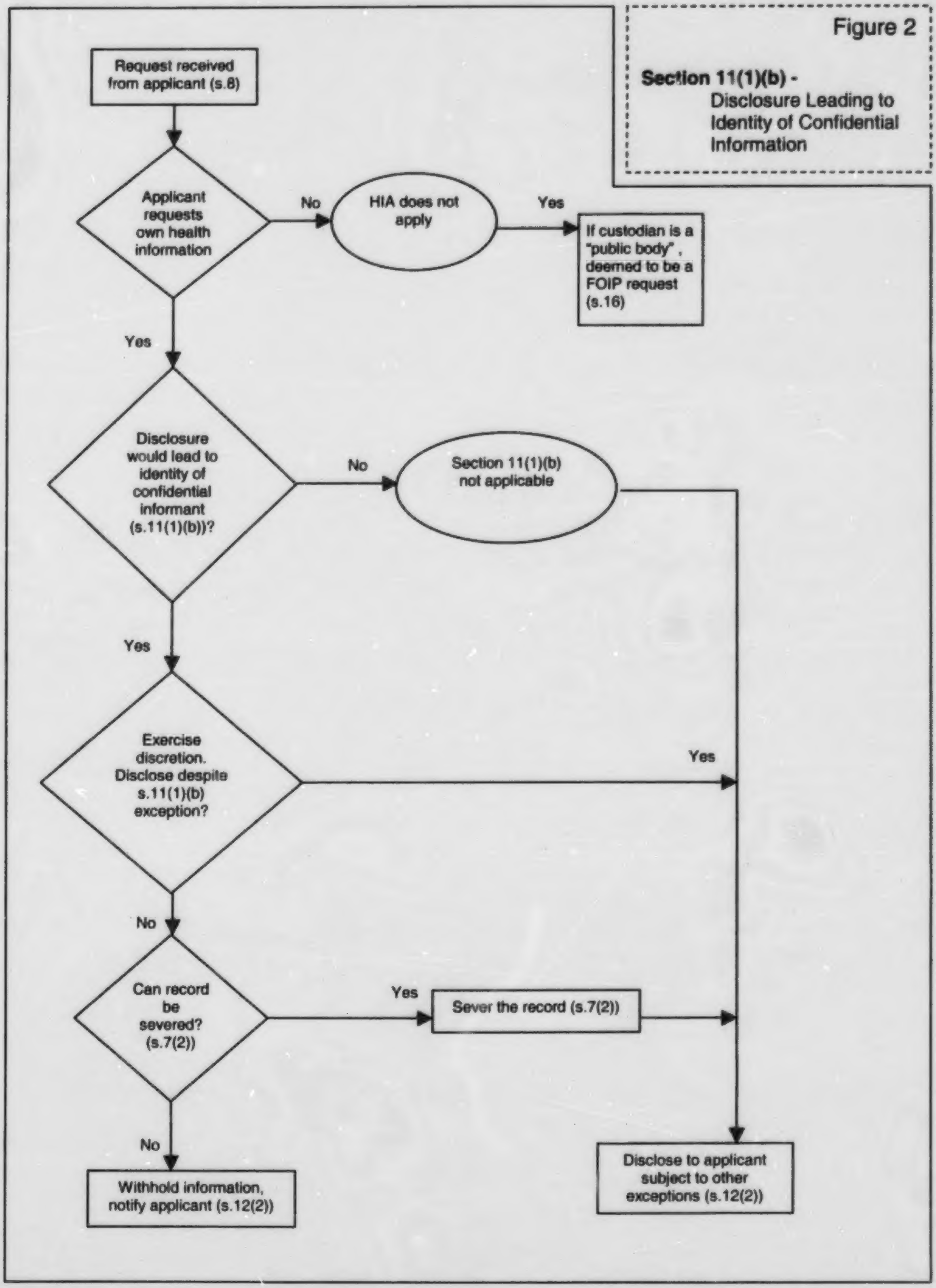


Figure 2

Section 11(1)(b) -
Disclosure Leading to Identity of Confidential Information

Request received from applicant (s.8)
Applicant requests own health information
No
HIA does not apply
Yes
If custodian is a "public body", deemed to be a FOIP request (s.16)
Yes
Disclosure would lead to identity of confidential informant (s.11(1)(b))?
No
Section 11(1)(b) not applicable
Yes
Exercise discretion. Disclose despite s.11(1)(b) exception?
Yes
No
Can record be severed? (s.7(2))
Yes
Sever the record (s.7(2))
No
Withhold information, notify applicant (s.12(2))
Disclose to applicant subject to other exceptions (s.12(2))

3.3.3 DISCLOSURE REVEALING ADVICE DEVELOPED BY OR FOR OR CONSULTATIONS INVOLVING A MEMBER OF EXECUTIVE COUNCIL

Section 11(1)(c) provides for a custodian to refuse to disclose health information if the disclosure could reasonably be expected to reveal:

- advice, proposals, recommendations, analyses or policy options developed by or for a member of the Executive Council; or
- consultations or deliberations involving a member of the Executive Council or the member's staff.

"Executive Council" means the group of Ministers and the Premier commonly known as the provincial Cabinet.

A **"member of Executive Council"** would be the Premier of Alberta, the Provincial Treasurer, the Ministers and the Associate Ministers.

This discretionary exception is intended to protect:

- the provision of advice by officials of the department to the Minister or to another member of Executive Council: and
- consultations or deliberations that may take place, involving the Minister or another member of Executive Council and a member of their staff.

It is intended to provide a "deliberative space" for those involved in providing advice, carrying on consultations and making recommendations so that records may be written with candour and cover all options.

This "deliberative space" is important for those involved in the policy making process. There is a need to preserve the relationship between members of Executive Council and those advising them as part of the overall accountability of custodians. A member of Executive Council may accept or reject the advice or recommendations developed by or for him or her and that person must be able to defend that decision.

Discretion is exercised by determining whether or not disclosure of a particular record or part of a record could reasonably be expected to reveal particular information about either the deliberative process itself or the matters being discussed. Release of information could also reveal the deliberative process implicitly if it allows an accurate inference to be made about that process.

The exercise of discretion should be based on the impact the disclosure can reasonably be expected to have on the custodian's ability to carry out similar internal decision-making processes in the future.

Consideration should be given to whether disclosure of the information in this instance would:

- make advisory processes less candid and comprehensive;
- make consultations or deliberations less frank; or
- hamper the policy-making process.

These determinations can only be made on a case by case basis, bearing in mind the magnitude of the process involved, the procedures for decision-making that have been followed, and the sensitivity of the particular information. A custodian should take into account the effect that disclosure would have on all steps of a decision-making process, not just the immediate interests regarding the particular information in question.

Advice, Proposals, Recommendations, Analyses or Policy Options

Section 11(1)(c)(i) is intended to protect candour in the giving of advice and formulation of proposals, analyses, policy options, recommendations, and related alternatives for potential courses of action that are developed by or for a member of the Executive Council.

It provides a zone of confidentiality around the policy-making process, rather than protecting all forms of advice **(see IPC Order 99-001).**

It applies to advice and recommendations obtained both from outside and inside the custodian, including those received under a contractual or other advisory arrangement.

"Recommendations" refers to formal recommendations about courses of action to be followed which are usually specific in nature and are proposed mainly in connection with a particular decision being made.

"Advice" refers to less formal suggestions about particular approaches to take or courses of action to follow.

"Proposals, Analyses or Policy Options" refer to the setting out of the advantages and disadvantages of particular courses of action.

"Member of Executive Council" would be a member of what is commonly known as the provincial Cabinet. The members consist of the Premier, the Provincial Treasurer, the Ministers and Associate Ministers.

Note that **section 11(1)(c)(i)** applies to advice given to the Premier, a Minister or Associate Minister acting alone. This discretionary exception is not to be confused with the mandatory exception related to revealing the substance of deliberations of Executive Council in **section 11(2)(c).**

The Information and Privacy Commissioner has defined these various terms as types of advice. The Commissioner's criteria for **"advice"** are that it should be:

- sought or expected, or be part of the responsibility of a person by virtue of that person's position;
- directed toward taking an action, including making a decision; and
- made to someone who can take or implement the action.

(See IPC Order 96-006 for further explanation of the definition of advice).

The Commissioner has determined that a statement of fact that is not directed toward action to be taken does not qualify as advice under this provision **(see IPC Order 97-007).**

However, if the factual information is sufficiently interwoven with other advice that it cannot reasonably be considered separate or distinct, it qualifies under this exception **(see IPC Order 99-001).**

This exception would not normally apply to the details of a study or background paper where factual information is presented. It is intended to apply to the information used to formulate possible directions in dealing with an issue or problem, to establish a policy or to make a decision.

The nature and significance of certain issues are such that disclosure of advice relating to them could reveal information that would damage the internal processes of decision-making within a custodian. Disclosure could also affect its overall ability to effectively manage programs and activities.

However, there are other issues where more openness surrounding the advisory and decision-making process can be of benefit. As well, there are also issues and activities of lesser significance where the disclosure of advice would have little or no effect on the overall administration or operation of the program or activity.

The wording of the exception in the *Health Information Act* is not as broad as the wording of a similar exception in **section 23(1)(a)** of the *FOIP Act.* That exception includes advice and recommendations developed by or for a public body as well as those developed by or for a member of Executive Council.

Consultations or Deliberations

Section 11(1)(c)(ii) allows a custodian to refuse access to those records or parts of records containing consultations or deliberations involving a member of Executive Council or the member's staff.

A **"consultation"** is a discussion or consideration where the views of one or more individuals or groups are sought about the appropriateness of particular proposals or suggested actions.

A **"deliberation"** is a discussion or consideration by a group of individuals of the reasons for and against a measure.

This exception would permit the frank exchange of views between a Minister and officials in his or her department who have been asked to provide advice or who have consultative responsibilities, or between a Minister and the Minister's staff.

Consultations and deliberations may involve the exchange of memoranda and proposals or may be part of agendas and minutes of meetings.

Individually identifying health information may have to be included in a briefing note to assist the Minister in responding to an issue. For example, a member of the public may be seeking payment for an experimental out-of-country treatment for a particular medical condition. This may be a complex issue with broader health policy implications and the individually identifying health information may be relevant to the Minister's decision.

The wording of the exception in the *Health Information Act* is not as broad as the wording of a similar exception in **section 23(1)(b)** of the *FOIP Act.* That exception includes consultations or deliberations involving officers or employees of a public body as well as those involving a Minister or a Minister's staff.

Figure 3 contains a flowchart setting out the steps for applying **section 11(1)(c).**

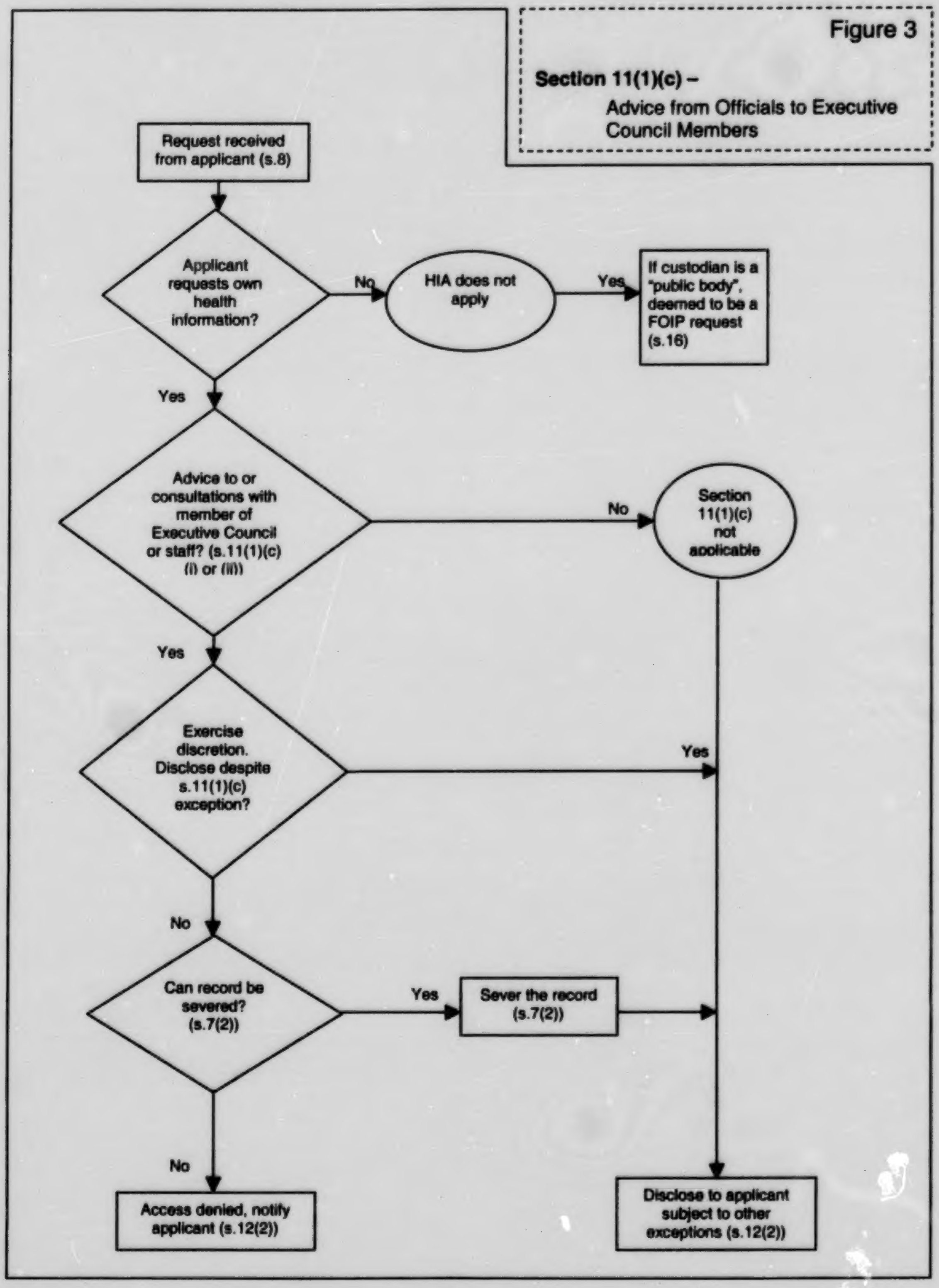


Figure 3
Section 11(1)(c) –
Advice from Officials to Executive Council Members
Request received from applicant (s.8)
Applicant requests own health information?
No
HIA does not apply
Yes
If custodian is a "public body", deemed to be a FOIP request (s.16)
Yes
Advice to or consultations with member of Executive Council or staff? (s.11(1)(c) (i) or (ii))
No
Section 11(1)(c) not applicable
Yes
Exercise discretion. Disclose despite s.11(1)(c) exception?
Yes
No
Can record be severed? (s.7(2))
Yes
Sever the record (s.7(2))
No
Access denied, notify applicant (s.12(2))
Disclose to applicant subject to other exceptions (s.12(2))

3.3.4 DISCLOSURE REVEALING ADVICE DEVELOPED BY OR FOR REGIONAL HEALTH AUTHORITIES OR PROVINCIAL HEALTH BOARDS

Section 11(1)(d) provides for a custodian to refuse to disclose health information if the disclosure could reasonably be expected to reveal advice, proposals, recommendations, analyses or policy options developed by or for the following custodians:

- a provincial health board established pursuant to regulations made under section 17(1)(a) of the *Regional Health Authorities Act* (e.g. the Alberta Mental Health Board);
- a regional health authority established under the *Regional Health Authorities Act; or*
- the Alberta Cancer Board continued under the *Cancer Programs Act.*

This discretionary exception is similar to the exception in **section 11(1)(c)** but in this case, it applies to the deliberative process within the types of custodians listed above. It is intended to protect candour in the giving of advice and the formulation of proposals, analyses, policy options, recommendations and related alternatives for potential courses of action that are developed by or for the custodians listed in the section.

It applies to advice and recommendations obtained both from outside and inside the custodian, including those received under a contractual or other advisory arrangement.

Discretion is exercised by determining whether disclosure of a particular record or part of a record could reasonably be expected to reveal particular information about either the deliberative process itself or the matters being discussed.

Consideration should be given to whether disclosure of the information in this instance would:

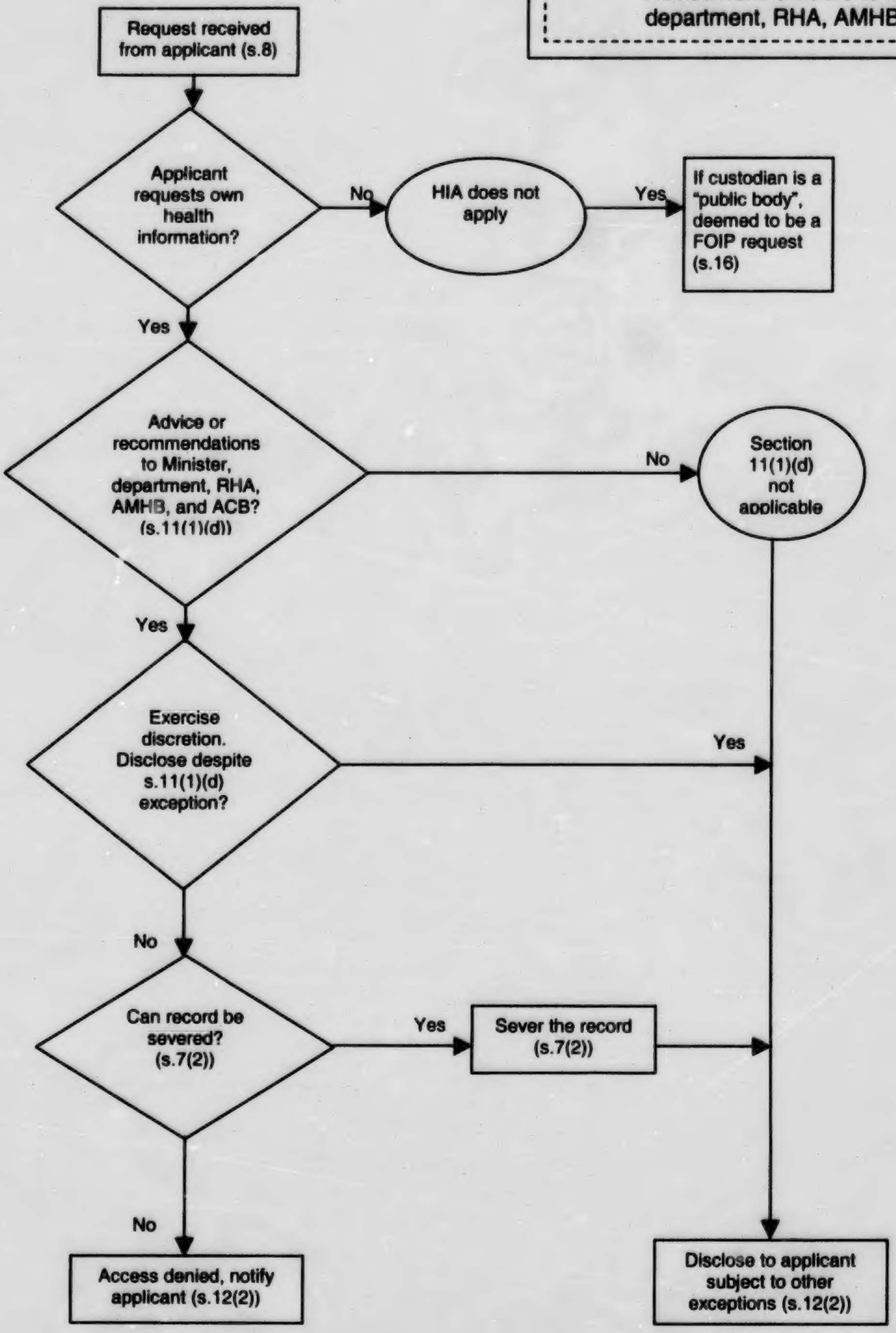
- make advisory processes less candid and comprehensive; or
- hamper the policy making process.

The exercise of discretion should be based on the impact the disclosure can reasonably be expected to have on the custodian's ability to carry out similar internal decision-making processes in the future.
(For a more detailed discussion on the application of this exception, see Section 3.3.3 of this Chapter, particularly the portion dealing with the application of section 11(1)(c)(i)).

Figure 4 contains a flowchart setting out the steps for applying **section 11(1)(d).**

Figure 4

Section 11(1)(d) –
Advice from Officials to Minister, department, RHA, AMHB and ACB


Request received from applicant (s.8)
Applicant requests own health information?
No
HIA does not apply
Yes
If custodian is a "public body", deemed to be a FOIP request (s.16)
Yes
Advice or recommendations to Minister, department, RHA, AMHB, and ACB? (s.11(1)(d))
No
Section 11(1)(d) not applicable
Yes
Exercise discretion. Disclose despite s.11(1)(d) exception?
Yes
No
Can record be severed? (s.7(2))
Yes
Sever the record (s.7(2))
No
Access denied, notify applicant (s.12(2))
Disclose to applicant subject to other exceptions (s.12(2))

3.3.5 DISCLOSURE PREJUDICING THE USE OR RESULTS OF AUDITS, DIAGNOSTIC TESTS OR ASSESSMENTS

Section 11(1)(e) provides that a custodian may refuse to disclose health information if it relates to:

- procedures or techniques relating to audits to be conducted or diagnostic tests or assessments to be given **(section 11(1)(e)(i))**;
- details of specific audits to be conducted or of specific tests or assessments to be given **(section 11(1)(e)(ii))**; or
- standardized diagnostic tests or assessments used by a custodian, including intelligence tests **(section 11(1)(e)(iii));**

and disclosure of the information could reasonably be expected to prejudice the use or results of particular audits, diagnostic tests or assessments.

This is a discretionary exception providing protection for the procedures and techniques involved in testing and auditing. It also protects details relating to specific tests to be given or audits to be conducted.

"Audit" means a financial, clinical or other formal or systematic examination or review of a program, portion of a program or activity **(section 1(1)(c).**

"Standardized diagnostic tests and assessments" could include psychological, aptitude or intelligence tests, among others.

Information is protected where disclosure of a test or audit that is to be conducted, or is currently in progress, would invalidate the results.

Information is also protected where there is an intention to use the procedure in the future, and disclosure would result in unreliable results being obtained and the test or audit having to be abandoned as a result. Test questions that are regularly used may be protected from disclosure.

Information relating to a test or audit that has been used in the past, but which is neither in progress nor will be used in the future, is not protected by this exception.

The exception applies to testing and auditing carried out both by the custodian and by consultants and contractors.

If the disclosure could reasonably be expected to prejudice the use or results of particular audits, diagnostic tests or assessments, custodians should exercise care in disclosing such results. For example, if revealing the details of a test or audit could lead to inaccurate results when the test is used in future, a custodian may wish to apply this exception.

Custodians should exercise care in disclosing the results of diagnostic tests or audits by ensuring that a professional familiar with the tests is available to explain and interpret them to the applicant. This process should be dealt with as part of a custodian's policies and procedures.

Figure 5 contains a flowchart setting out the steps for applying **section 11(1)(e).**

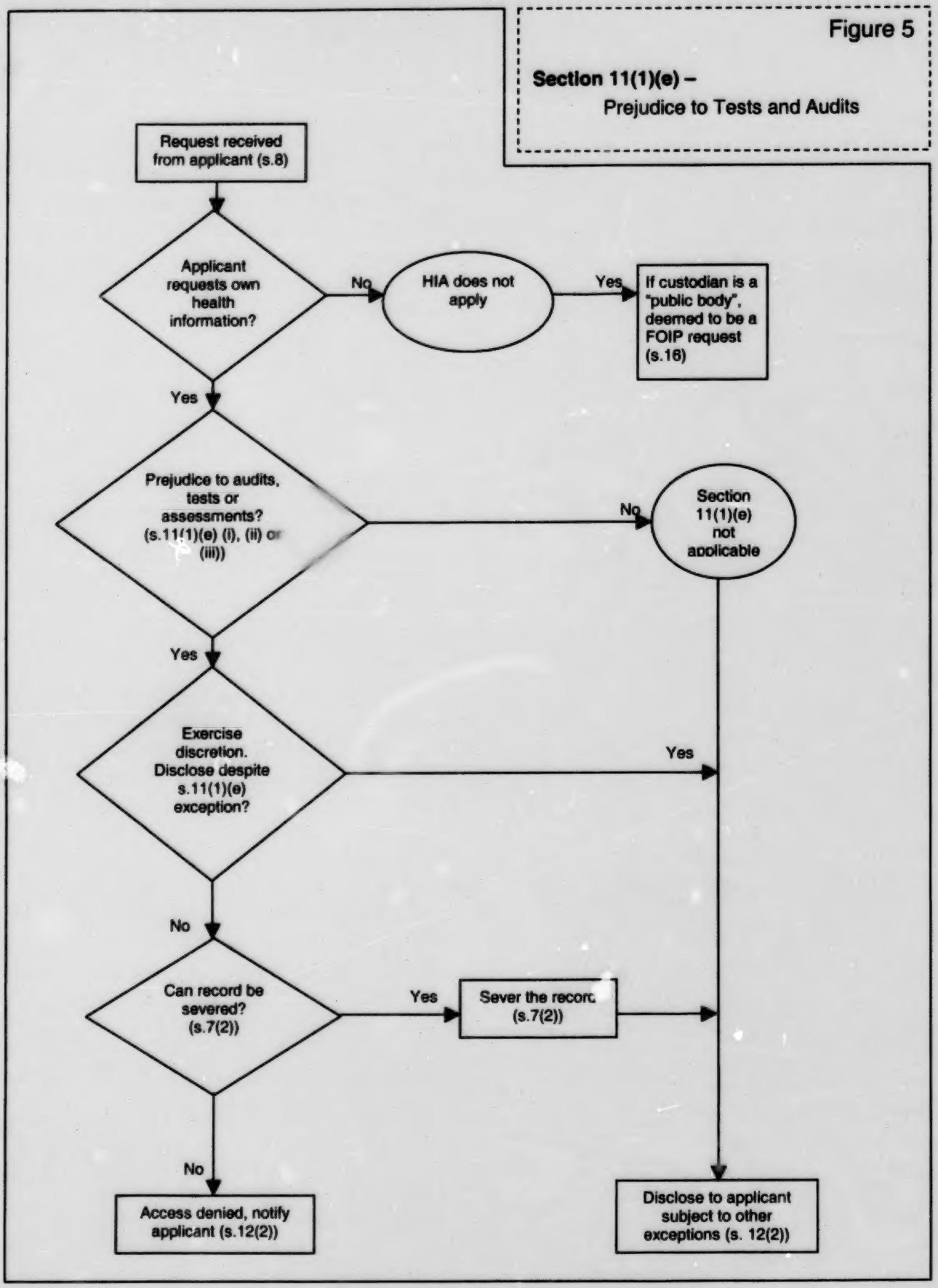


Figure 5

Section 11(1)(e) –
Prejudice to Tests and Audits

Request received from applicant (s.8)
Applicant requests own health information?
No
HIA does not apply
Yes
If custodian is a "public body", deemed to be a FOIP request (s.16)
Yes
Prejudice to audits, tests or assessments? (s.11(1)(e) (i), (ii) or (iii))
No
Section 11(1)(e) not applicable
Yes
Exercise discretion. Disclose despite s.11(1)(e) exception?
Yes
No
Can record be severed? (s.7(2))
Yes
Sever the record (s.7(2))
No
Access denied, notify applicant (s.12(2))
Disclose to applicant subject to other exceptions (s. 12(2))

3.4 MANDATORY EXCEPTIONS

3.4.1 DISCLOSURE OF INFORMATION ABOUT AN INDIVIDUAL OTHER THAN THE APPLICANT

Section 11(2)(a) requires a custodian to refuse to disclose health information to an applicant if the health information is about an individual other than the applicant, unless the health information was originally provided by the applicant in the context of a health service being provided to the applicant.

If all or part of the information requested by the applicant falls within this exception, the custodian has no discretion to disclose the information.

This mandatory exception is different than the mandatory exception regarding disclosure of third party personal information in **section 16(1) of the *FOIP Act*. Section 11(2)(a) of the *Health Information Act*** does **not** require a custodian to determine whether the disclosure of health information would be an unreasonable invasion of another individual's personal privacy.

Section 11(2)(a) is more categorical. If health information about another individual is part of the record(s) requested by an applicant, and the health information was not provided by the applicant in the context of a health service being provided to the applicant, the custodian would have to sever that information from the record before the record was disclosed to the applicant.

There may be situations where an applicant has provided health information about family members or other relatives to his or her physician in the context of providing a medical history. The information about other individuals provided by the applicant as part of their medical history, could be disclosed to the applicant requesting access to his or her health information.

Figure 6 contains a flowchart setting out the steps for applying **section 11(2)(a).**

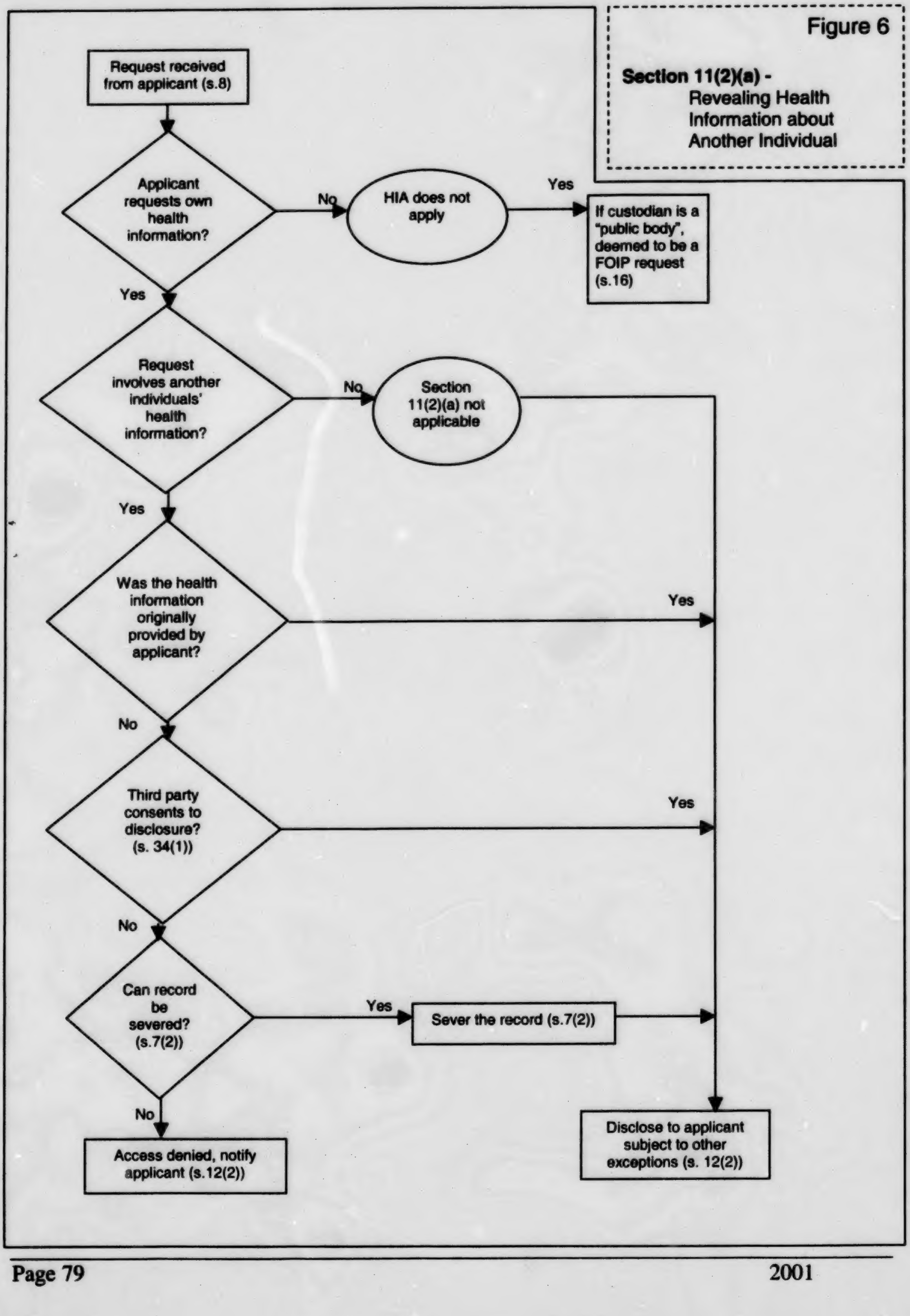


Figure 6

Section 11(2)(a) - Revealing Health Information about Another Individual

Request received from applicant (s.8)
Applicant requests own health information?
No
HIA does not apply
Yes
If custodian is a "public body", deemed to be a FOIP request (s.16)
Yes
Request involves another individuals' health information?
No
Section 11(2)(a) not applicable
Yes
Was the health information originally provided by applicant?
Yes
No
Third party consents to disclosure? (s. 34(1))
Yes
No
Can record be severed? (s.7(2))
Yes
Sever the record (s.7(2))
No
Access denied, notify applicant (s.12(2))
Disclose to applicant subject to other exceptions (s. 12(2))

3.4.2 DISCLOSURE OF PROCEDURES OR RESULTS OF AN INVESTIGATION OF A HEALTH SERVICES PROVIDER

Section 11(2)(b) creates a mandatory exception for the disclosure of information that sets out procedures or contains the results of an investigation, a discipline proceeding, a practice review or an inspection relating to a health services provider.

"Investigation" refers to a systematic process of examination, inquiry and observation.

"Discipline proceeding" refers to a formal process of determining whether a practitioner has displayed a lack of skill or judgment in the practice of his or her profession; has displayed unbecoming and/or unprofessional, disgraceful or dishonourable conduct; or is incapable or unfit to practice his or her profession.

"Practice review" refers to an assessment or evaluation of the professional performance or competence of a practitioner.

"Inspection" refers to the examination or viewing of the physical premises or of the books, records, papers or other documents of a practitioner as part of an investigation.

"Procedures" refers to the methods and processes by which the examinations, inquiries and observations are carried out and include the equipment and technology employed in those activities.

Both the procedures and the results of an investigation of a health services provider, or of a discipline proceeding, a practice review or an inspection relating to a health services provider fall within this mandatory exception.

Refusal to disclose information that sets out the procedures for such activities relates to the need to maintain the continued effectiveness of the investigative techniques and procedures used or likely to be used in the investigative activity.

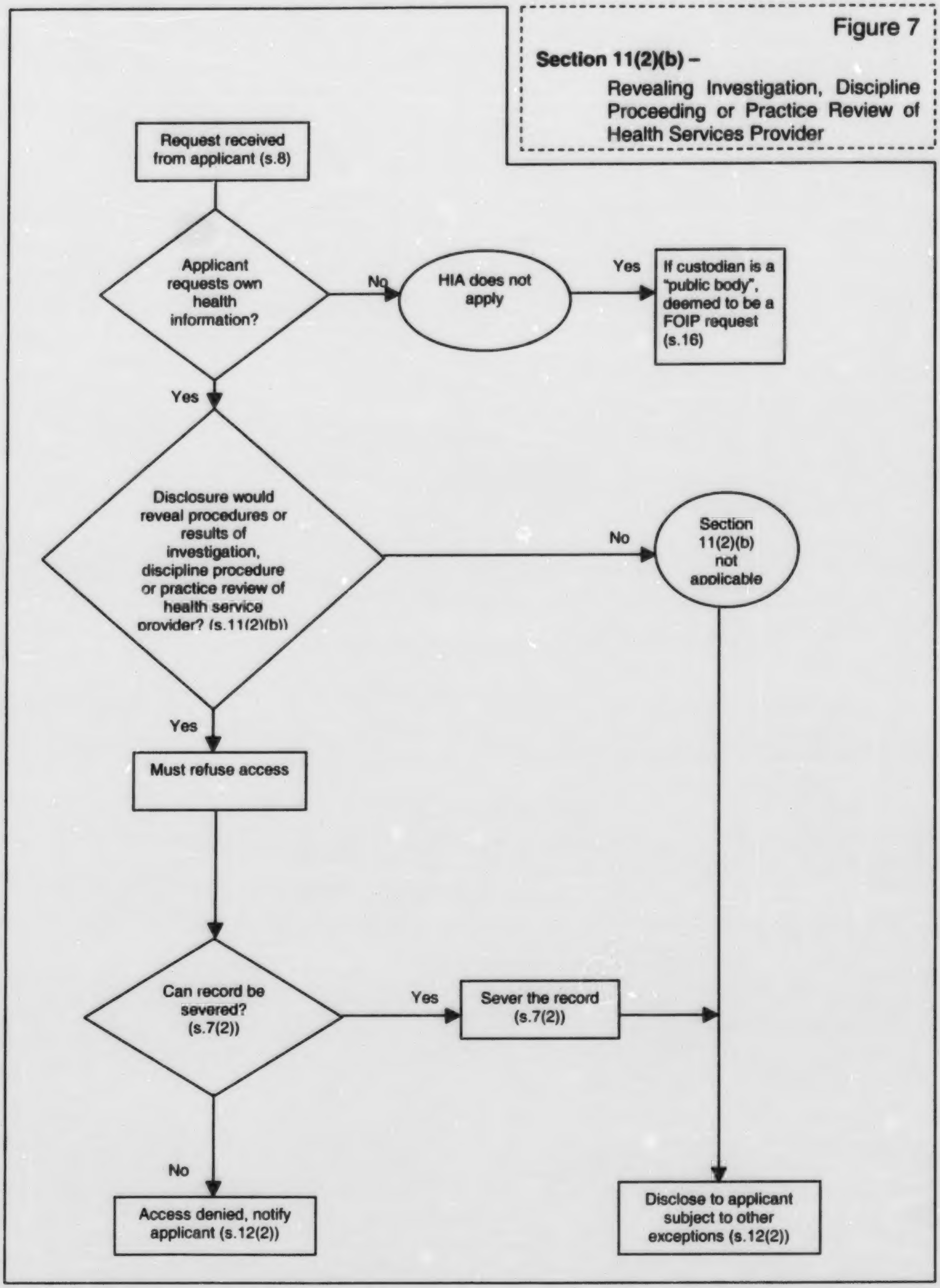
The results of investigations or disciplinary proceedings, etc. involving a health services provider are not disclosed because the disciplinary processes and disclosure of information about them are governed by other professional legislation. Those processes are carried out by the provider's professional association.

Figure 7 contains a flowchart setting out the steps for applying **section 11(2)(b).**

Figure 7

Section 11(2)(b) –

Revealing Investigation, Discipline Proceeding or Practice Review of Health Services Provider


Request received from applicant (s.8)
Applicant requests own health information?
No
HIA does not apply
Yes
If custodian is a "public body", deemed to be a FOIP request (s.16)
Yes
Disclosure would reveal procedures or results of investigation, discipline procedure or practice review of health service provider? (s.11(2)(b))
No
Section 11(2)(b) not applicable
Yes
Must refuse access
Can record be severed? (s.7(2))
Yes
Sever the record (s.7(2))
No
Access denied, notify applicant (s.12(2))
Disclose to applicant subject to other exceptions (s.12(2))

3.4.3 DISCLOSURE REVEALING SUBSTANCE OF DELIBERATIONS OF EXECUTIVE COUNCIL OR TREASURY BOARD

Section 11(2)(c) creates a mandatory exception that prohibits the disclosure of health information that would reveal the substance of deliberations of the Executive Council or any of its committees or of the Treasury Board or any of its committees.

The information subject to the exception includes any advice, recommendations, policy considerations or draft legislation or regulations submitted or prepared for submission to the Executive Council or any of its committees or to the Treasury Board or any of its committees.

"Advice, recommendations" refers to the analysis and presentation of various options for a suggested course of action that is the subject of deliberation. The advice or recommendation must deal with issues that will be, are or have been discussed by the Executive Council, Treasury Board or one of the committees of either body.

"Policy considerations" refers to analysis and flagging of issues that deserve special consideration by ministers when taking action or making policy decisions at Executive Council, Treasury Board or a committee of either.

"Executive Council" means the group of Ministers and the Premier acting collectively as the provincial Cabinet. This exception does not apply to a minister acting alone, unless the individual minister is carrying out the direction of Cabinet or is acting as a Cabinet committee.

"Committees of Executive Council or Cabinet committees and committees of the Treasury Board" include the Agenda and Priorities Committee, Treasury Board committees and other ad hoc committees struck to deal with specific issues.

This exception is based on the convention of collective ministerial responsibility to the Legislature and to Albertans for the actions of the government. In order to facilitate this collective decision-making, Cabinet discussions and deliberations have traditionally been kept confidential. This permits full and frank discussions.

There may also be situations where Cabinet may wish to delay public announcement of its decisions. It may have entered into arrangements with affected individuals to postpone an announcement of a decision until a specific time.

Cabinet may also develop plans to deal with issues, emergencies or contingencies. The value of these plans would be lessened if immediate access to the plans were granted.

Because **section 11(2)(c)** deals with the Cabinet process, the Office of the Executive Council makes all decisions relating to disclosure of submissions to the Executive Council and related records. Alberta Treasury makes all decisions relating to disclosure of submissions to Treasury Board and related records. In the case of Treasury Board confidences, this approval requirement does not extend to records that Treasury Board requires the department to prepare, such as a business plan.

Consultations regarding these types of records must be conducted with Executive Council, for Cabinet confidences and with Alberta Treasury, for Treasury Board confidences.

Substance of Deliberations

Custodians must determine whether a record or part of a record reveals the substance of the deliberations of the Executive Council, the Treasury Board or any of their committees, either explicitly or implicitly.

A release of information **"explicitly"** reveals the substance of deliberations if the information itself contains the essence of the discussion or deliberations or reveals the contents of the deliberations.

A release of information **"implicitly"** reveals this type of information if it is reasonable to expect that disclosed information could be combined with other information to reveal the substance of Executive Council, Treasury Board or their committee deliberations.

"Substance" means the essence or essential part of a deliberation.

"Deliberation" means the act of weighing and examining the reasons for and against a contemplated act or course of conduct. It also includes an examination of choices of direction or means to accomplish an objective.

It is possible that special case or precedent setting situations may end up being discussed by Executive Council from a policy perspective or by Treasury Board from a financial perspective. While it would generally be possible to discuss these matters using non-identifying health information, sometimes the high profile public nature of the case (e.g. a person out of country requesting payment for health-related costs, or a person requesting to travel out of country for a health service, in unusual circumstances) means that that the identity of the individual will be readily known.

Individuals have a right to access any record containing health information about them. While an individual's health records will not be forwarded to Executive Council or Treasury Board, records may contain references to particular health information about an identifiable individual.

Examples of Records

Examples of records that would reveal the substance of deliberations of the Executive Council, Treasury Board or one of their committees are:

- agendas, minutes and related documents of Executive Council meetings;
- letters and memoranda concerning issues deliberated upon or the decisions or directions taken by ministers but not made public which may have been sent to ministerial colleagues or senior public servants;
- briefing material, exclusive of background facts, placed before Executive Council, Treasury Board or one of their committees;
- a memorandum (including electronic mail) from the Secretary to Cabinet to ministers discussing Cabinet decisions;
- a memorandum (including electronic mail) from a deputy minister to an assistant deputy minister or chief executive officer or other senior officer dealing with issues that will be or have been deliberated upon by the Executive Council, Treasury Board or one of their committees;
- a record of discussions between senior officials about issues that will be or have been deliberated upon by the Executive Council, Treasury Board or one of their committees; and

- a draft or final submission to Executive Council or Treasury Board, excluding background facts.

When the Exception Does Not Apply

The exception in **section 11(2)(c)** does not apply where the health information:

- has been in existence for 15 years or more **(section 11(2)(c)(i))**;
- is part of a record of a decision made by the Executive Council or any of its committees on an appeal under an Act **(section 11(2)(c)(ii))**; or
- is part of a record the purpose of which is to present background facts to the Executive Council or any of its committees or to the Treasury Board or any of its committees for consideration in making a decision where:
  - the decision has been made public
  - the decision has been implemented; or
  - 5 years or more have passed since the decision was made or considered **(section 11(2)(c)(iii))**.

Where the Executive Council or one of its committees functions as an appeal body under an Act and makes a decision, the decision and any recorded reasons for the decision are available to the public **(section 11(2)(c)(ii))**.

Other portions of the record, such as the advice and recommendations supporting the process leading to a decision remain subject to **section 11(2)(c)**.

Section 11(2)(c)(iii) permits the release of information prepared specifically with the intent of presenting factual information to the Executive Council, Treasury Board or any of their committees.

"Background facts" means facts that provide explanatory or contributory information or circumstances. These are usually found in attachments to submission documents and are intended to assist in the Cabinet deliberations.

A **"decision has been made public"** if it has been communicated to the public in an authorized way. This would include communication in a statement by a minister, a statement during Question Period, a presentation in the Legislative Assembly, or a letter, statement or news release to the media. A "leak" of information is not considered an authorized disclosure of information.

A **"decision has been implemented"** if the decision has been put into effect or acted upon even if the implementation or action is not complete. A decision is not considered to have been implemented if it remains subject to approval or is not final.
When a decision is reconsidered, clarified, amended, reversed or delayed, the exception does not apply to background facts if the decision subsequently reconsidered has either been made public or implemented. However, other provisions of the *Act* may prevent disclosure.

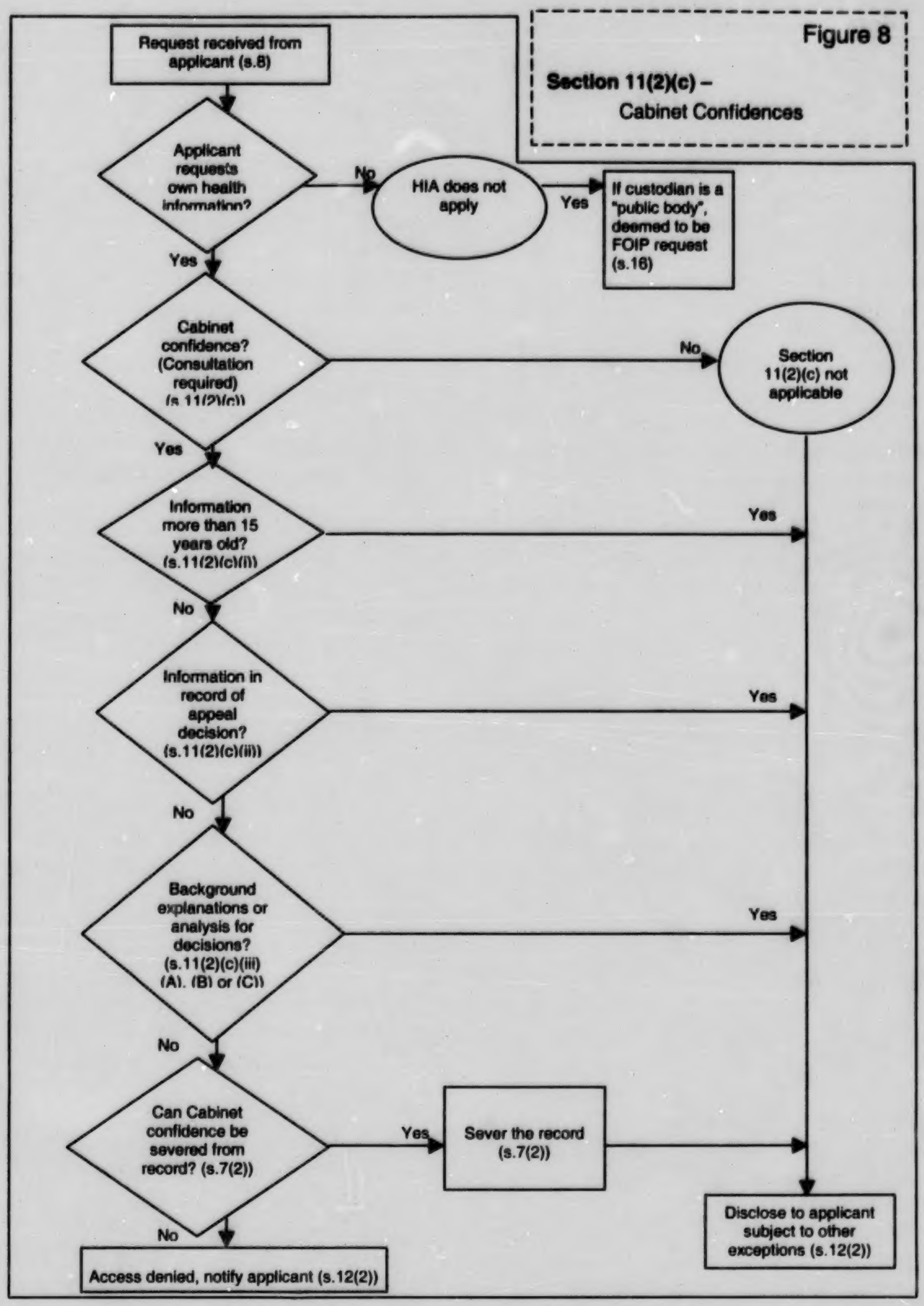
In applying **section 11(2)(c)(iii),** the context in which a record containing background facts was presented to Executive Council or Treasury Board must be examined. Just because a decision on a particular subject has been made public does not mean that background facts respecting a related decision can be disclosed. One must consider what decision was being deliberated when the background facts were submitted to Cabinet. **(See IPC Order 97-010).**

"More than 5 years have passed since the decision was made or considered" means 5 years from a particular month and day to a corresponding month and day 5 years later. This condition applies regardless of whether a decision has been made public or has been implemented.

Figure 8 contains a flowchart setting out the steps for applying **section 11(2)(c).**

Figure 8

Section 11(2)(c) –
Cabinet Confidences


Request received from applicant (s.8)
Applicant requests own health information?
No
HIA does not apply
Yes
If custodian is a "public body", deemed to be FOIP request (s.16)
Yes
Cabinet confidence? (Consultation required) (s.11(2)(c))
No
Section 11(2)(c) not applicable
Yes
Information more than 15 years old? (s.11(2)(c)(i))
Yes
No
Information in record of appeal decision? (s.11(2)(c)(ii))
Yes
No
Background explanations or analysis for decisions? (s.11(2)(c)(iii) (A), (B) or (C))
Yes
No
Can Cabinet confidence be severed from record? (s.7(2))
Yes
Sever the record (s.7(2))
No
Access denied, notify applicant (s.12(2))
Disclose to applicant subject to other exceptions (s.12(2))

3.4.4 DISCLOSURE PROHIBITED BY ANOTHER ENACTMENT OF ALBERTA

Section 11(2)(d) creates a mandatory exception to the disclosure of health information where the disclosure would be expressly prohibited by another Alberta act or regulation.

Certain acts and regulations, or sections of acts or regulations may state that they prevail despite the *Health Information Act* **(see section 11(2)(d))**. If another act or regulation or section of an act or regulation states that the disclosure of certain health information is prohibited, **section 11(2)(d)** would require a custodian to refuse to disclose the requested health information to an applicant.

Examples of provisions in statutes that prohibit the disclosure of health information would be:

- **section 11(1)** of the *Human Tissue Gift Act* which precludes the disclosure of information that could identify the donor or recipient of an organ; and
- **section 9** of the *Alberta Evidence Act*, which creates a statutory privilege to prohibit disclosure of a "quality assurance record" as defined under that *Act*.

The *Alberta Evidence Act* prohibits a witness in an action from producing any quality assurance record in the possession or control of that person or in the possession or control of a quality assurance committee **(section 9(2)(b))**.

A **"quality assurance record"** includes 'a record of information in any form that is created or received by or for a quality assurance committee in the course of or for the purpose of its carrying out quality assurance activities' **(section 9(1)(c) of the** *Alberta Evidence Act***)**.

A **"quality assurance committee"** is defined in the *Alberta Evidence Act* as a body with the primary purpose of carrying out quality assurance activities, which is appointed, established or designated in accordance with **section 9(1)(b)** of that *Act*.

It should be noted that a quality assurance record as defined under **section 9** of the *Alberta Evidence Act* is not a record to which the *Freedom of Information and Protection of Privacy Act* applies. This means that an applicant that is refused access to a quality assurance record under the *Health Information Act* could not successfully make an application for access under the *FOIP Act* **(section 4(1)(b.1)** of the *FOIP Act*).

Incident Reports

An incident report in and of itself is **not** a quality assurance record. Quality assurance reports may contain patient records or health information about an individual that has been derived from an incident report. These records, however, only provide the raw data or material for a quality assurance report.

The *Alberta Evidence Act* does not apply to original medical and hospital records relating to a patient **(section 9(3)** of that *Act*.)

Whether custodians will be able to refuse access to Incident Reports will have to be determined on a case by case basis and will depend upon the practice of the custodian respecting these records and the facts in each situation.

An individual making an access request may argue that he or she is entitled to access the health information contained in an Incident Report, which is in the custody of a custodian pursuant to **section 7(1)** of the *Health Information Act*.

However, a custodian may argue that the main purpose of an Incident Report is to describe an unexpected incident and prevent future incidents, rather than to describe health services provided to a particular individual.

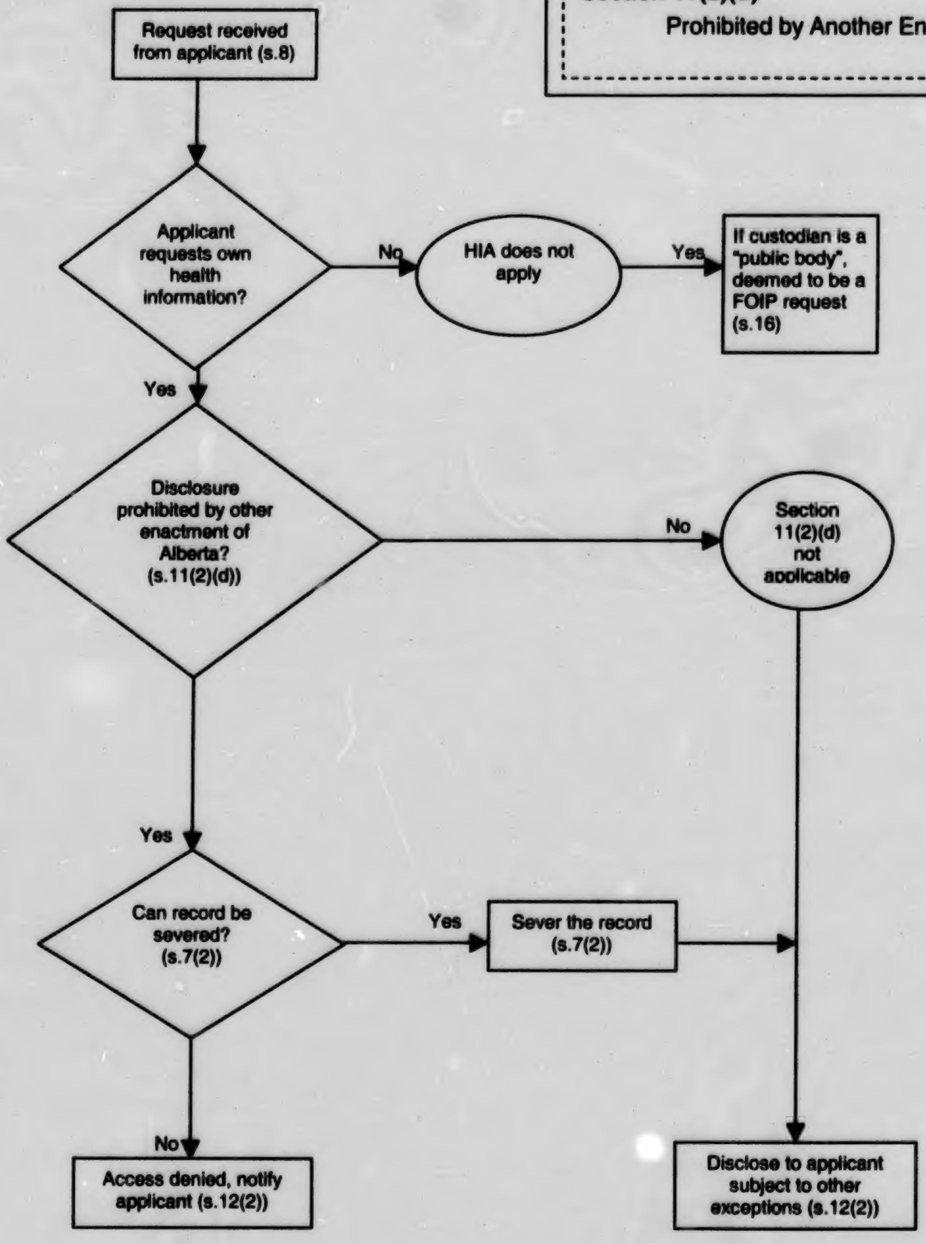
The custodian would have the onus or burden of proof to show that the person making the request has no right of access to the health information.

Some health care facilities keep Incident Reports as a part of the hospital record. The *Nursing Homes Operation Regulation*, **AB Reg. 258/85**, has a unique requirement for long term care facilities to keep unusual occurrence reports as part of the resident's record **(section 11(1)(i)(iii))**. This practice and statutory requirement weigh in favour of the argument that an Incident Report contains health information that should be disclosed to an individual requesting access.

Figure 9 contains a flowchart setting out the steps for applying **section 11(2)(d).**

Figure 9

Section 11(2)(d) –
Prohibited by Another Enactment


Request received from applicant (s.8)
Applicant requests own health information?
No
HIA does not apply
Yes
If custodian is a "public body", deemed to be a FOIP request (s.16)
Yes
Disclosure prohibited by other enactment of Alberta? (s.11(2)(d))
No
Section 11(2)(d) not applicable
Yes
Can record be severed? (s.7(2))
Yes
Sever the record (s.7(2))
No
Access denied, notify applicant (s.12(2))
Disclose to applicant subject to other exceptions (s.12(2))

THINGS TO REMEMBER

RIGHT TO REFUSE ACCESS TO HEALTH INFORMATION

DISCRETIONARY EXCEPTIONS

A custodian **may** refuse to disclose all or part of the health information in a record that falls within a discretionary exception under *section 11(1)* of the *Act* but must determine whether the record should be disclosed even though it might qualify for the exception. The discretionary exceptions are used where disclosure of the information would:

- harm individual health or safety or threaten public safety;
- revealing the identity of a confidential source of health information;
- revealing advice developed by or for or consultations involving a member of Executive Council;
- revealing advice developed by or for a health authority, a provincial health board or Alberta Cancer Board; or
- prejudicing the use or results of audits or tests.

MANDATORY EXCEPTIONS

A custodian **must** refuse to disclose all or part of the health information in a record if the information falls within a mandatory exception under *section 11(2)* of the *Act*. The mandatory exceptions are used where disclosure of the information would:

- reveal information about individuals other than the applicant;
- reveal procedures or results of investigation of a health services provider;
- revealing the substance of deliberations of Executive Council or Treasury Board; or
- be prohibited by another enactment of Alberta.

INCONSISTENCY OR CONFLICT WITH ANOTHER ENACTMENT

If a provision of the *Health Information Act* is inconsistent or in conflict with a provision of another act or regulation, the provision of the *Health Information Act* prevails unless the other act or a regulation under the *Health Information Act* expressly says that the other act, or regulation or a provision of it, prevails over the *Health Information Act* (see Chapter 12 on Paramountcy and Consequential Amendments)

APPLYING THE EXCEPTIONS

- Review the record(s) to determine if any of the exceptions in the *Health Information Act* may apply and to identify information where no exception applies.
- Review the record(s) to determine if the release of the records is inconsistent or in conflict with another act or regulation. If the records being reviewed have a direct relationship to a provision of another act or regulation that expressly prevails over the *Health Information Act,* the release of information is subject to the provisions of the other act.
- Where discretion is permitted, decide whether all or part of the information subject to the exception will be released or refused.
- Sever the part of the record(s) to which the custodian has decided that access needs to be refused.
- Prepare a response to the applicant indicating the reason for refusal of all or part of the requested information.
- The exercise of discretion must be reasonable and not arbitrary, adapted to the circumstances of the request at hand, non-discriminatory and consistent.
- For help in applying the exceptions, refer to the flow chart diagrams following the discussion of each exception in the Manual.

CHAPTER FOUR

CORRECTION OR AMENDMENT OF HEALTH INFORMATION

4.1 OVERVIEW OF CHAPTER FOUR

This Chapter will cover:

- the meaning of a request for correction or amendment of health information;
- how an individual may make a request to correct or amend the individual's own health information;
- how a custodian should respond to a request to correct or amend an individual's health information;
- agreeing to make a correction or amendment to health information;
- refusing to correct or amend health information;
- time limits for responding to requests;
- deemed requests under the *FOIP Act; and*
- administering the correction/amendment process.

4.2 HOW DOES AN INDIVIDUAL REQUEST A CORRECTION TO OR AMENDMENT OF THE INDIVIDUAL'S HEALTH INFORMATION?

Section 2(d) provides individuals with the right to request correction or amendment of health information about themselves.

"Correction" refers to the process of removing a mistake or error in a health record and replacing it with what is right or accurate.

"Amendment" refers to the process or changing or varying something in a health record.

Under **section 13(1),** an individual who believes that there is an error or omission in the individual's health information may make a written request to the custodian whom he or she believes has the information in its custody or under its control to correct or amend the information.

An **"error"** refers to mistaken or wrong information or information that does not reflect the true state of affairs.

An **"omission"** refers to information that is incomplete or missing or that has been overlooked.

A custodian has **"custody"** of health information when it is in the possession of the custodian and the custodian has a right to deal with the information.

A custodian has **"control"** of health information when it has the authority to manage the health information in such ways as restricting, regulating and administering its use, disclosure and disposition.

See Chapter 2, section 2.3 of this Publication for a further discussion of custody and control.

"Health information" is defined in **section 1(1)(k)** to mean diagnostic, treatment and care information **(section 1(1)(i))**; health services provider information **(section 1(1)(o))**; and registration information **(section 1(1)(u)).**

4.2.1 NATURE AND FORM OF REQUEST

The request must be submitted in writing to the custodian whom the applicant believes has custody or control of the health information in dispute. The applicant may use the *Request to Correct or Amend Health Information Form* found in **Appendix 1 of this Publication** or use a letter to request that the correction or amendment be made.

An applicant must provide proof or evidence in support of the request for correction or amendment. The proof should be of the same nature and at least the same quality as was required when the original information was collected. For example, a birth or baptismal certificate might be needed to prove an individual's age for eligibility for certain benefits. Reports of x-ray or laboratory tests or document showing a medical diagnosis might be needed to prove that a certain medical condition exists; or academic diplomas or certificates could prove certain competencies or educational qualifications of a health services provider.

Note that there are no fees required to be paid by an applicant who is requesting a correction or amendment to his or her own health information.

4.2.2 HOW DOES A CUSTODIAN RESPOND TO A REQUEST FOR CORRECTION OR AMENDMENT OF HEALTH INFORMATION?

Within the time limits set out in **section 13** or any extended period under **section 15**, a custodian must decide whether it will make or refuse to make a correction or amendment to health information **(section 13(2)).**

4.2.3 AGREEING TO MAKE A CORRECTOIN OR AMENDMENT

When a custodian agrees to make a correction of an error or to amend health information, all records containing the health information in question must be corrected. This includes records in all forms and formats – paper, electronic and microform. When a custodian agrees to add omitted health information, all records containing the health information in any form or format must be updated to add the omitted information.

In addition to making the correction or amendment, the custodian must:

- give written notice to the applicant that the correction or amendment has been made; and
- notify any person to whom the information has been disclosed during the one-year period before the correction or amendment was requested, that the correction or amendment has been made **(section 13(3)).**

This is one of the reasons why a custodian must make a notation of the disclosure of a record containing diagnostic, treatment and care information **(section 41)**.

Making the Correction or Amendment

The requested correction or amendment is made by noting it on the record containing the health information, close to the information under challenge. The notation should be signed and dated. When designing electronic forms and databases, care should be given to allow for this kind of notation process.

In cases where health information is stored on a medium such as microform, a linking process may have to be used to update the information. To **"link"** a record means to attach, join or connect the record to the requested correction or amendment. This may consist of a letter or statement from the applicant or a copy of the *Request to Correct or Amend Health Information Form.*

The custodian must ensure that the new information is stored and retrieved with the original information whenever the information is used for an administrative purpose directly affecting the individual involved. In addition, the notation of the correction or amendment must be made available to the individual should he or she request access to his or her health information **(see IPC Order 97-020)**.

Notifying the Applicant

The custodian must give the applicant written notice of its decision. **Model Letter I in Appendix 2 of this Publication** may be used to notify the applicant that the correction or amendment has been made. A copy of the corrected or amended record should be attached or the applicant advised of the name and address of the appropriate office where the corrected or amended record can be inspected.

Notifying Other Persons

Section 13(3)(c) requires a custodian to inform any person to whom the health information has been disclosed, that the correction or amendment has been made. Notification must be given to any person who has received the information within one year prior to the request for correction or amendment. This ensures that other parties have accurate and complete information for their own decision-making processes.

Notification of other persons is not necessary if:

- the custodian believes that the applicant will not be harmed if the notification is not provided; and
- the applicant agrees **(section 13(4))**.

To ensure that the applicant is advised and agrees with the custodian's assessment, the applicant should consent in writing to dispensing with notification. **Model Letter K in Appendix 2** may be used to advise the applicant and request the applicant's consent to dispensing with notification of other persons.

Routine Requests

For routine corrections or amendments, such as a change of name, address, etc., there is no need to follow the formal request for correction process under the *Act*. However, the custodian should follow its own procedure regarding the proof that the applicant needs to provide before the correction or amendment is made.

4.2.4 REFUSING TO MAKE A CORRECTION OR AMENDMENT

If a custodian refuses to make the requested correction or amendment, it must, within the time limits in **section 13** or any extended time periods under **section 15,** notify the applicant in writing that the request has been refused and provide reasons for the refusal **(section 13(5))**.

Notifying the Applicant

The custodian must give the applicant written notice of its decision. **Model Letter I in Appendix 2 of this Publication** may be used to notify the applicant of the refusal to make the requested correction or amendment. In the notice, the custodian must also tell the applicant that he or she may ask the Commissioner to review the custodian's decision or submit a statement of disagreement.

Grounds for Refusal

A custodian may refuse or may be unable to make a requested correction or amendment because it is not satisfied with the proof presented by the applicant.

In addition to refusing because of lack of satisfactory proof, **section 13(6)** permits a custodian to refuse to make a correction or amendment in respect of:

- a professional opinion or observation made by a health services provider about the applicant **(section 13(6)(a))**; or
- a record that was not originally created by that custodian **(section 13(6)(b))**.

Section 13(6)(a) recognizes that the significance of an opinion may be that it reflects another person's view at the time it was offered. It may be important to have a record of that view or assessment at a later date. **Section 14(1)(b)** allows an individual to have his or her views about that opinion added to the record for other readers to consider.

If the health information requested to be corrected or amended is in a record that was not created by the custodian receiving the request **(section 13(6)(b)**, the applicant may be referred to the custodian who did create the record if their identity can be determined from the record.

Request for Review or Submission of Statement of Disagreement

Under **section 14(1)**, if a custodian refuses to make a correction or amendment, the custodian must tell the applicant that he or she may elect to do either of the following **but not both:**

- ask the Commissioner to review the custodian's decision; or
- submit a statement of disagreement.

Under **section 73(1)**, an individual may ask the Commissioner to review a custodian's decision to refuse to correct or amend health information. A request for review must be in writing and must follow the requirements in **section 74.**

A **"statement of disagreement" (in section 14(1)(b))** means a statement from the applicant setting out in 500 words or less the requested correction or amendment and the applicant's reasons for disagreeing with the decision of the custodian.

On receiving the statement of disagreement, the custodian must:

- if reasonably practicable, attach the statement to the record that is the subject of the requested correction or amendment; and
- provide a copy of the statement of disagreement to any person to whom the custodian has disclosed the record in the one-year period prior to the applicant's request for correction or amendment **(section 14(3))**.

This is similar to the notification requirement with which custodians must comply in **section 13(3)(c)**. **Model Letter I in Appendix 2** can be used for this purpose.

4.2.5 TIME LIMITS FOR RESPONDING

Agreeing or Refusing to Make a Correction or Amendment

Under **section 13(2),** a custodian must decide to make or refuse to make the requested correction or amendment within 30 days after receiving the request or within any extended period under **section 15.**

Deemed Refusal

If the custodian fails to respond to a request for correction or amendment in accordance with **section 13** within 30 days or within any extended period under **section 15,** it is treated as a decision to refuse to make the correction or amendment **(section 13(7)).** The applicant can ask the Commissioner to review the decision to refuse under **section 73(1).**

Submission of Statement of Disagreement

Section 14(2) states that an applicant who elects to submit a statement of disagreement must submit the statement to the custodian within 30 days after the written notice of refusal has been given to the applicant under **section 13(5)** or within any extended period under **section 15(3).**

Request for Review

Under **section 74(2),** a request for the Commissioner to review a custodian's decision to refuse to make a correction or amendment must be in writing and must be delivered to the Commissioner within 60 days after the applicant is notified of the decision, or any longer period allowed by the Commissioner **(section 74(2)).**

In the case of a deemed refusal under **section 13(7),** the time limit for requesting a review would not apply.

4.2.6 EXTENDING TIME LIMITS

Under **section 15(1),** the custodian may extend the time for responding to a request under **section 13(1)** for an additional period of up to 30 days or, with the Commissioner's permission, for a longer period if:

- the request does not give enough detail to enable the custodian to identify the record that is to be corrected or amended;
- a large number of records are involved in the request and responding within the period set out in **section 13(2)** would unreasonably interfere with the operations of the custodian; or
- more time is needed to consult with another custodian before deciding whether to make the correction or amendment requested.

Notifying the Applicant

If the time is extended, the custodian must tell the applicant:

- the reason for the extension;
- when a response can be expected; and
- that the applicant may make a complaint to the Commissioner about the extension under **section 85 (section 15(2))**

See Chapter 10 of this Publication for a further discussion on the Commissioner's power to resolve complaints.

Model Letter B in Appendix 2 of this Publication deals with time extensions for access requests and can be modified for a request for correction or amendment. This notice is required as soon as it is apparent that the request cannot be processed within the initial 30-day time period.

Under **section 15(3)**, the Commissioner may extend the time within which an applicant must submit the statement of disagreement under **section 14(2)** if, in the Commissioner's opinion:

- it is unreasonable to expect the applicant to submit the statement within the 30 day period set out in **section 14(2)**; or
- it is fair to extend the time for any other reason.

As was the case for extending the time limit for responding to an access request, a custodian should consider all factors relating to the possibility of the need for a time extension before deciding to invoke one. Common factors include:

- the amount and type of detail needed from the applicant to clarify the request;
- the breadth and complexity of the request, the number of records requested and the number of files or sites which must be searched to find the requested records. Extensions cannot be claimed for consultations within the custodian (i.e. with other affiliates) after the records have been located;
- the number and complexity of consultations required with other custodians or levels of government; and
- the quantity and type of records requiring review by other custodians.

Limits on Extensions

Custodians should make every effort to plan the processing of complicated requests for correction or amendment so that there is a need to invoke only one extension.

If a custodian believes that responding to the request will require more than a total of 60 days (the original 30 days plus the extended 30 day period), it should ask the Commissioner for permission to extend the time limit beyond the original 30 days. This must be done in writing and normally within the original 30 day time limit.

A letter to the Commissioner requesting the extension should set out the specific conditions relating to the request which will necessitate a period greater than 60 days for its processing and establish a reasonable period (e.g. 90 days) for producing a response.

In exceptional circumstances, a custodian who has already taken a 30 day extension, may seek a second extension from the Commissioner. This might occur when the relevant records suddenly involve complications not originally contemplated when planning the response process. Where the Commissioner refuses to grant permission for an extension, the custodian has only a maximum of 60 days to process the request. Custodians must continue to process a request while awaiting the Commissioner's response to an extension request.

Custodians must document the reasons for a time limit extension. This documentation will help support the custodian's decision to extend the time limit for 30 days; will provide a rationale for asking the Commissioner to extend the time limit for more than 30 days; and will help in situations where the applicant has complained to the Commissioner about the extended time limit.

When a request for extension is made to the Commissioner, the notice should be sent to the applicant before the Commissioner's final decision on the extension has been made.

If an applicant complains to the Commissioner about an extension, the custodian continues to process the request throughout the review period.

After investigating a complaint about a time limit extension, the Commissioner may either confirm or reduce the extension of a time limit as provided in **section 80(3)(b).**

Day of Response

The Alberta *Interpretation Act* provides that, if the day a response is due falls on a statutory holiday or a day when the office of the custodian that is authorized to receive requests under the *Health Information Act* is closed, then the response is due on the next business day. The custodian is responsible for determining whether the office that is authorized to respond is closed. If a small or single custodian's office is closed for staff vacations, the completion of the request will be affected and can legitimately be delayed until the first working day after the office reopens.

4.2.7 DEEMED REQUESTS FOR CORRECTION OR AMENDMENT UNDER THE *FOIP ACT*

If a written request for correction or amendment of health information is made under **section 13(1)**, and the record contains information that would be subject to the *FOIP Act*, the request is deemed to be a request under **section 35 of the *FOIP Act*** and that *Act* applies to the request as if it had been made under **section 35(1)** of the *FOIP Act* **(section 16(2))**.

This section does not apply if the custodian that receives the request is not a "public body" as defined in **section 1(1)(p)** of the *FOIP Act* **(section 16(3))**. However, the section would apply, for example, to a regional health authority, the Alberta Mental Health Board and the Alberta Cancer Board which are custodians under the *Health Information Act* and are also public bodies under the *FOIP Act*.

The applicant must be told that the request will be processed under the *FOIP Act* and whether this will affect the timelines for responding. **Model Letter H.1 of Appendix 2 of this Publication** can be used to notify the applicant that the request is being deemed a FOIP request under the *FOIP Act*.

Since the provisions for processing requests for correction or amendment under the *FOIP Act* are very similar to those under the *Health Information Act*, the impact of applying the *FOIP Act* to the request should be minimal from the applicant's perspective.

Section 35.2 of the *FOIP Act* states that if a request is made under **section 35(1)** of that *Act* to correct personal information that contains information to which the *Health Information Act* applies, the part of the request that relates to that information is deemed to be a request under **section 13(1)** of the *Health Information Act* and that *Act* applies as if the request had been made under **section 13(1)** of the *Health Information Act*.

This section does not apply if the public body that receives the request is not a custodian as defined in **section 1(1)(f)** of the *Health Information Act*.

4.3 ADMINISTERING THE CORRECTION OR AMENDMENT PROCESS

Custodians should develop procedures to process requests for correction or amendment and to ensure that processing occurs within established time limits and in accordance with the requirements of the *Health Information Act.*

4.3.1 RECEIPT AND LOGGING OF REQUEST

Once a request is received by a custodian (either in the authorized office of the Health Information Coordinator of a large or decentralized custodian or in the authorized office of a single or smaller custodian), it should be registered and logged. This could be done electronically if an automated tracking system is in use.

It should then be placed in a request for correction file and details of the request forwarded to the office or program area of a custodian that has custody or control of the health record(s) in dispute. The office of the Coordinator can record the assignment of responsibility on the request tracking system.

The identity of the applicant will be needed to locate and retrieve records containing the disputed health information but should be disclosed only:

- to those officials and employees of the custodian who have a need to know it in order to carry out their job duties; and
- to the extent necessary to carry out the custodian's function in processing the applicant's request.

4.3.2 CLARIFYING THE REQUEST

If a request does not sufficiently describe the records sought to be corrected or amended, a custodian should advise the applicant and offer to help clarify or narrow the request. **Model Letter H in Appendix 2** can be used in this situation.

If an applicant has requested a large number of corrections the Health Information Coordinator should try to narrow the request while still meeting the applicant's needs. This could result in provision of better service, in terms of both time and results.

If the scope of a request for correction has been changed, the custodian should document the change and send a notice to the applicant **(see Model Letter I in Appendix 2).**

4.3.3 ACKNOWLEDGING THE REQUEST

The custodian should acknowledge receipt of a request. This acknowledgment may say that the request:

- has been received and processing will commence;
- is not clear or precise enough and more information is needed to clarify it before processing can commence; or
- contains information that is subject to the *FOIP Act.* That part of the request is deemed to be a request for correction under the *FOIP Act.* The applicant should be told how that part of the request will be dealt with.

If processing cannot start immediately, an effort should be made to contact the applicant by telephone to resolve any problems quickly. A written follow-up to this call is good practice. It will provide a definite reference point as to when processing commenced.

Model Letter H in Appendix 2 sets out the options for acknowledging receipt of a request for correction or amendment.

4.3.4 LOCATING AND RETRIEVING RECORDS

A custodian must make every reasonable effort to respond to a request for correction or amendment of health information openly, accurately and completely. Normally, the area responsible for the custody or control of records relevant to a request would be asked to locate and retrieve the records.

This responsibility may rest with the medical records technician or medical records unit of a health facility or clinic or it may rest with a staff member of a physician's or pharmacist's office.

In most cases, an applicant will be asking for correction or amendment of a specific record or specific information in a database, so the record or information should be able to be retrieved within a reasonably short period of time. For example, the applicant's records indicate that he or she has no drug allergies when, in fact, he or she is allergic to penicillin.

An applicant can ask the Information and Privacy Commissioner to review the adequacy of a search to locate records **(section 85(a))**. When this happens, the custodian will have to demonstrate that it made a reasonable search of all areas and repositories where records relevant to the request for correction might be located.

(See IPC Order 96-022 for the criteria the Commissioner uses in judging the adequacy of a search for records).

Custodians must not dispose of any records relating to a request after it is received, even if the records are scheduled for destruction under an approved records retention and disposition schedule. This includes any E-mail and transitory records relevant to the request that may exist at the time the request is received. The receipt of a request under **section 13(1)** freezes all disposition activity relating to the records covered by the request until the request has been completed, the time period for any appeal to the Commissioner has elapsed or an appeal has been decided.

Where records have been destroyed prior to the receipt of a request, in accordance with an approved records retention and disposition schedule, the custodian's response to the applicant should indicate that the records have been destroyed, quoting the authority for, and date of destruction.

When records have been transferred to the Provincial Archives of Alberta (in the case of the department), or to the archives of a custodian, the applicant may be referred to the archives.

4.3.5 COPYING RETRIEVED RECORDS

Once the records have been located, either the program area in a larger custodian or the office of the Health Information Coordinator, as appropriate, prepares them for review in terms of the correction or amendment and completes the request documentation.

This may involve the copying and numbering of all records pertinent to the request and preparing:

- a list of all records areas searched; and
- a list of the records located in each records area, along with identifying data and parts of file lists, data dictionaries or other finding aids used in locating the records.

4.3.6 REVIEWER'S RECOMMENDATIONS

The Health Information Coordinator or other individual responsible for reviewing the requested record(s) recommends whether a correction or amendment should be made or refused. This recommendation forms the basis for a discussion between a physician or pharmacist and the staff member who reviewed the request and the record(s) or between the Coordinator and decision - maker in a larger custodian.

At this stage, any legal advice needed to resolve issues arising from the request should be sought. Any interpretive or policy issues which need to be raised should be identified and consultation undertaken. A written memo of the reviewer's recommendations should contain:

- a summary of file systems, offices and records storage facilities searched;
- copies of records relevant to the request; and
- a written summary of recommendations for making or refusing to make the correction or amendment, including any background information to explain decisions.

The memo should be approved by whomever the custodian has designated as the responsible person to approve requests for correction or amendment.

4.3.7 DOCUMENTING AND TRACKING REQUESTS FOR CORRECTION OR AMENDMENT

Custodians should maintain documentation systems to record all deliberations and decisions regarding the processing of requests for correction or amendment and to help ensure that the request process meets the requirements set out in the *Act*.

The documentation may become a critical part of the evidence required during a review by the Information and Privacy Commissioner. It can also be of assistance in processing subsequent similar requests **(see IPC Order 99-011).**

The 30 day time period for responding to requests starts on the day after receipt of a request for correction in the office of the custodian designated to receive such request. In a large or decentralized custodian, this would normally be the office of the Health Information Coordinator. A request may be delivered to any office of a custodian during normal business hours, but the time limit for responding does not start until the request is received in an office authorized to receive requests.

Custodians need to have a reasonable system in place to ensure that requests are forwarded immediately to the office(s) designated to receive and begin processing them.

Reasonable steps might include special forwarding instructions to staff in mail rooms or to staff who open the mail, as well as use of a color-coded transmittal file to indicate the priority and important nature of the request. Staff should be made aware of the urgent nature of requests under the *Health Information Act* and the need to forward them immediately to the Health Information Coordinator or person designated as responsible for responding to requests.

Once the request is received in the authorized office, it should be date-stamped.

Custodians may establish an automated or manual tracking system depending upon the volume of work generated by requests under the *Act*. Tracking systems help ensure that the time periods under the *Act* are complied with and keep track of progress in responding to a request. Automated systems are not normally needed unless a custodian receives more than 50 requests annually (including access requests) or the custodian is decentralized and there is a need to coordinate responses. Database software, such as Microsoft Access could be used to develop an automated tracking system for requests.

4.3.8 MAINTAINING COPIES OF REQUESTS AND RECORDS

***BEST PRACTICE:** Custodians should keep a file for each request for correction or amendment processed under the Act. This file should include:*

- *all internal and external correspondence, including a copy of the original request from the applicant, any notices sent to the applicant and any other correspondence from the applicant;*
- *an unmarked copy of the record(s) retrieved and reviewed in response to a request;*
- *a copy of the corrected or amended record(s) or a notation of the refusal to correct or amend and the reasons for this;*
- *a copy of a statement of disagreement from the applicant (if any); and*
- *any other information documenting the request management process*

This practice helps support the custodian in any review by the Information and Privacy Commissioner.

4.3.9 CLOSURE AND RETENTION OF REQUEST FILES

It is a good practice to keep a request for correction or amendment file active for at least 60 days after responding to a request in order to allow time for a request for a review by the Commissioner. If a review is requested, the file will be reopened and remain open until the review process is complete.

Once the file is closed, either because the custodian has responded to the request, a review has been completed, or a request has been declared to be abandoned, the custodian must retain the request file for the period of time authorized by its retention and disposition schedule. Custodians must not transfer, store or destroy request records except in accordance with such authorization.

4.3.10 ABANDONMENT OF REQUESTS

Sometimes applicants will indicate in writing or by telephone an intention not to proceed with a request. This may be because they have changed their mind or because they feel they no longer need the information corrected or amended.

However, an applicant may simply cease to respond during the processing of a request. When this situation occurs, **section 9** sets out the provisions for declaring a request to be abandoned. The custodian must have contacted the applicant in writing to seek further information necessary to process the request.

If the applicant does not respond within 30 days of being contacted, the custodian can advise the applicant, in writing, that the request for correction or amendment has been declared abandoned as of a specific date. This notice must state that the applicant can ask for a review of the decision by the Commissioner.

In some cases, an applicant abandons a request after processing is completed. For example, an applicant may have asked to pick up the corrected/amended records and does not do so. If the custodian:

- has responded to the applicant's request, stating whether the correction or amendment will be made or refused;
- has indicated where and when the record(s) may be picked up; and
- the applicant does not respond or pick up the records within 30 days

the custodian can advise the applicant that the request has been declared abandoned. The file should be kept active for a further 60 days in order to allow time for the applicant to request a review by the Commissioner.

Model Letter D in Appendix 2 deals with this type of situation for access requests and can be modified for requests for correction or amendment.

THINGS TO REMEMBER

CORRECTION OR AMENDMENT OF HEALTH INFORMATION

Written Request

- An individual has a right to make a written request asking that a correction or amendment be made to their own health information.
- A request for correction or amendment of health information must be submitted in writing to the custodian whom the applicant believes has custody or control of the health information in dispute. The applicant may use the Request to Correct or Amend Health Information Form (in Appendix 1 of the Manual) (section 13(1)).

Routine Requests

- For routine corrections such as a change of name, address, etc., there is no need to follow the formal request for correction process under the *Act* but the custodian should follow its own procedures regarding the required proof needed to make the correction or amendment.

Time Limits

- A request for correction or amendment of health information must be responded to by the custodian within 30 calendar days unless the time limit has been extended in accordance with the *Act* (section 13(2) and (3)).

No Cost

- There are no fees for processing a request for correction or amendment.

Model Letters

- For help in processing a request, refer to the Model Letters (in Appendix 2 of the Manual).

Agreeing to Make the Correction

- If the custodian agrees to correct or amend health information, all records containing the information must be corrected or updated and the custodian must notify any person to whom the information has been disclosed during the prior one-year period that the correction or amendment has been made (section 13(3)).

Refusal to Correct

- A custodian may refuse to make a correction or amendment if there is lack of satisfactory proof, if the record was not originally created by that custodian or if the correction or amendment deals with a professional opinion or observation made by a health services provider about the applicant (section 13(6)).

Review by Commissioner

- If the custodian refuses to make the correction or amendment, the applicant must be told that he or she may either ask the Commissioner to review the custodian's refusal or submit a statement of disagreement in 500 words or less (section 14).

Deemed Request under the *FOIP Act*

If a request for correction or amendment contains information that would be subject to the *FOIP Act*, the rules under the *FOIP Act* apply to the request (section 16(2)).

CHAPTER FIVE

DUTIES AND POWERS OF CUSTODIANS RELATING TO HEALTH INFORMATION

5.1 OVERVIEW OF CHAPTER FIVE

This Chapter will cover:

- the duty of custodians to only collect, use and disclose the minimum amount of health information with the highest degree of anonymity;
- the duty of custodians to ensure the accuracy of health information; identify affiliates that are responsible for ensuring compliance with the *Act* and regulations and for establishing or adopting policies and procedures to facilitate the implementation of the *Act* and regulations;
- the duty of custodians to maintain administrative, technical and physical safeguards to protect the privacy of individuals and the confidentiality of their health information;
- the duty of custodians to obtain an individual's consent before information is disclosed by electronic means;
- the duty of custodians to do privacy impact assessments whenever new administrative practices and information systems relating to the collection, use and disclosure of individually identifying health information are being proposed;
- the power of custodians to charge a fee for providing copies of an individual's health record;
- the power of custodians to transform health information to create non-identifying health information;
- the power of custodians to enter agreements with "information managers"; and
- the rules that custodians must follow for data matching.

5.2 GENERAL DUTIES OF CUSTODIANS

The duties of custodians are set out in **Part 6 of the *Act*** and encompass a set of fair information practices for health information. Fair information practices are universally understood by organizations that are subject to access and privacy legislation such as the Alberta *Freedom of Information and Protection of Privacy Act.*

Under the *Health Information Act*, the collection, use and disclosure of health information must, in all cases, be carried out in the most limited manner and with the highest degree of anonymity that is possible in the circumstances **(section 2(c)).** This fundamental purpose of the *Act* applies throughout the *Act* to all custodians, including the Minister and the department.

The other duties of custodians set out in **Part 6** of the *Act* **(Duties and Powers of Custodians Relating to Health Information)** relate to another fundamental purpose of the *Health Information Act* as listed in **section 2(a)**, namely the establishment of strong and effective mechanisms to protect the privacy and confidentiality of an individual's health information.

5.2.1 DUTY TO COLLECT, USE AND DISCLOSE HEALTH INFORMATION WITH THE HIGHEST DEGREE OF ANONYMITY POSSIBLE

The decision by a custodian to collect, use or disclose "individually identifying health information" (the most sensitive level of information) should only be made after considering whether "aggregate" or other "non-identifying" health information would adequately achieve the intended purpose.

Under **section 57(2),** custodians are expected to first consider whether the collection, use or disclosure of "aggregate health information" (the least sensitive level of information) would be adequate for the intended purpose. If that is the case, the custodian must collect, use or disclose only "aggregate health information".

If "aggregate health information" is not adequate for the intended purpose, the custodian must then consider whether other "non-identifying health information" (the middle level of sensitivity of information) would be adequate for the intended purpose. If that is the case, the custodian may collect, use or disclose other "non-identifying health information" **(section 57(3)).**

If "aggregate" and other "non-identifying health information" is not adequate for the intended purpose, the custodian may collect, use or disclose "individually identifying health information" if the collection, use or disclosure:

- is authorized by the *Act;* and
- is carried out in accordance with the *Act* **(section 57(4)).**

"Aggregate health information" means non-identifying health information about groups of individuals with common characteristics. This is often referred to as statistical information and often is the kind of information from which it is virtually impossible to identify a single individual, unless the cell or sample size is very small (less than 10). An example of aggregate health information would be a regional health authority in a large urban region disclosing to a researcher the number of caesarian sections performed in that region on women over the age of 25.

"Non-identifying health information" means that the identity of the individual who is the subject of the information cannot be readily ascertained from the information **(section 1(1)(r)).** By removing an individual's name and personal identifiers before information is disclosed from information or records that were identifiable, and by not providing other contextual information, the information could essentially become anonymous individual or non-identifying information.

"Individually identifying health information" means that the identity of the individual who is the subject of the information can be readily ascertained from the information **(section 1(1)(p)).** This type of information would include personal identifiers such as an individual's name, address, birth date, full postal code, personal health number, and so on.

"Readily ascertained" in the context of **section 57**, means that the identity of an individual (e.g. the individual's name or other identifiers or distinguishing characteristics associated with an individual) can be determined or deduced without having to apply a sophisticated technical method or process, or without having any particular technical expertise to do so.

The identity of an individual can be said to be "readily ascertained" if:

- the identity can be determined by combining available data or information within the same or in several different records held by one custodian;
- the identity can be determined by comparing information representing distinguishing characteristics with other information sources having both the distinguishing characteristics and the names or other identifiers of individuals; and
- if only readily available or conventional computer hardware, software and technical expertise is used.

Need to Know

The "need to know" principle is expressed in **sections 24, 28 and 43**. These sections require affiliates of custodians to collect, use or disclose health information in a manner that is in accordance with that affiliate's duties to the custodian.

Section 24 states that an affiliate of a custodian must not collect health information in any manner that is not in accordance with the affiliate's duties to the custodian. Under **section 28**, an affiliate of a custodian must not use health information in any manner that is not in accordance with the affiliate's duties to the custodian.

Section 43 expresses a similar requirement regarding disclosure. Under that section, an affiliate of a custodian must not disclose health information in any manner that is not in accordance with the affiliate's duties to the custodian.

Applying this principle to **section 57,** an employee with an administrative or policy role for a custodian should not necessarily have access to individually identifying health information since there would be no need for him or her to use health information in that form.

When Principle of Highest Degree of Anonymity Does Not Apply

Custodians do not have to apply this "continuum" of highest degree of anonymity to the collection, use or disclosure of health information for the purpose of providing "health services" **(as defined in section 1(1)(m))**, or for determining or verifying the eligibility of an individual to receive a "health service" **(section 57(5))**.

5.2.2 DUTY TO COLLECT, USE AND DISCLOSE HEALTH INFORMATION IN A LIMITED MANNER

In addition to complying with **section 57**, custodians must also collect, use or disclose only the amount of health information that is essential to enable the custodian, or the recipient of the information, to carry out the intended purpose **(section 58(1))**.

Not all of the health information created and maintained by a custodian is relevant or necessary to carry out a certain purpose or address a request for information. Even if a custodian is required by the *Act* to disclose health information, it should be done by disclosing the least amount possible to achieve the intended purpose.

For example, a physician would not release a patient's complete file without knowing who the information is being disclosed to, why it is needed and whether the same purpose could be achieved by releasing less information. Even if the *Act* requires the disclosure of individually identifying health information, the personal health number, date of service and a code indicating the type of service might be sufficient.

Need to Know

The "need to know" principle, expressed in **sections 24, 28 and 43 (see discussion under 2.3.1)**, also applies to **section 58(1)**. Affiliates of custodians may only collect, use and disclose the least amount of health information necessary to achieve their intended purpose. Even employees or others involved in direct patient care should only have access to information about the patients they are responsible for or providing care to.

Expressed Wishes of Individual

In deciding how much health information to disclose, a custodian must consider any expressed wishes of the individual who is the subject of the information, together with any other factors the custodian considers relevant (**section 58(2)**). An example of a relevant factor that could override the expressed wishes of an individual might be the need for a psychiatrist to have a full and complete medical and psychiatric history of an individual in order to treat a current mental illness of the individual even if the individual does not wish to divulge any of this information.

The power to "transform" individually identifying health information to create non-identifying health information in **section 65** is discussed later in this **Chapter under section 5.4.1.** Anonymity transformation may be used to support the requirements set out in **sections 57 and 58.**

5.2.3 DUTY TO OBTAIN CONSENT BEFORE DISCLOSING DIAGNOSTIC, TREATMENT AND CARE INFORMATION BY ELECTRONIC MEANS

Section 59 requires a custodian to obtain an individual's consent, or ensure that consent was previously obtained, before disclosing individually identifying diagnostic, treatment and care information by electronic means (**section 59(1)**).

"Electronic means" is defined in **section 1(2)** of the Health Information Regulation as a computer system that facilitates access by authorized persons to electronic or digital information that is stored in a computer database by a custodian.

In plain language, this means that a custodian must obtain consent (or ensure that consent has been previously obtained) before disclosing individually identifying diagnostic, treatment and care information that will be obtained by accessing a database through a computer network.

This section does not apply where the disclosure of individually identifying diagnostic, treatment and care information is for the purpose of obtaining or processing payment for health services (**section 59(7)**). For example, if a physician is sending billing information about a patient electronically in order to process a payment for providing health services, consent for this disclosure is not required. Likewise, if a pharmacist is processing a claim for payment of a prescription for a client, through a health benefits insurance carrier, a **section 59** consent is not required.

When custodians communicate diagnostic, treatment and care information by "person-to-person communication", they must follow the collection, use and disclosure rules in the *Health Information Act*. They may disclose the information to each other without the individual's consent, provided the information is to be used for a **section 27** purpose (e.g. to provide patient care) and that the least amount of information is disclosed at the highest level of anonymity. They must also protect the privacy of the individuals who are the subjects of the information being disclosed and the confidentiality of their health information.

Custodians are free to use any method to disclose information on a person-to-person basis. That includes face-to-face verbal communication, telephone, video, writing, fax, e-mail, Intranet or Internet communication. With person-to-person communications, the *Health Information Act* relies on each custodian to manually oversee the transfer of information between them according to the rules in the *Act*.

With automated computers and networks, custodians can access information that has been stored in a computer database by another custodian via a network. In this case, the computer software, and not a person, discloses the information. The software oversees the transfer of information by incorporating the collection and disclosure requirements of the *Act*. The main risks of using automated computers and networks relate to user accountability and security. When custodians place information in a computer database, they do not know when it will be accessed through the network and by whom. Instead, they must rely on the assumption that only authorized users will access the information according to the pre-agreed rules in the software.

The benefits of using automated computer databases and networks to communicate information are that:

- individuals can access information when they need it, not when the other individual can provide it; and
- accountability and security provisions (such as audit trails) can be built into the software governing the network that are more rigorous than those for paper-based information systems. These provisions should address risks that could arise from inappropriate disclosure of information via the automated network.

Once a custodian obtains an individual's consent to disclose information by "electronic means", the custodian will not place all of the individual's information in the computer databases. Economic constraints will limit the data elements for the Pharmaceutical Information Network. The summary information will contain significant provisions that need to be protected, but will not contain detailed clinical notes.

An information manager, such as alberta we//net in the case of the Pharmaceutical Information Network, will actively maintain the automated computers and network and their software to ensure that security and accountability provisions are up to date and that authorized users can be held accountable for their behavior.

Although fax, e-mail, Intranet and Internet communications use computers in the communication process, they are excluded from the definition of "electronic means" because they rely on custodians specifically directing the transfer of information to another custodian. Stakeholders also indicated that including e-mail, Intranet and Internet communications in the definition of "electronic means" would place an inappropriate administrative burden on custodians because these new forms of communication are rapidly replacing more traditional forms of person-to-person communication. Obtaining consent for their use would be onerous.

An example of disclosure by electronic means is the Breast Cancer Screening Program which is part of the promoting health and well-being strategy of alberta we//net. This program will establish a consistent, province-wide approach to conducting mammograms for the purpose of screening for breast cancer. alberta we//net provides the technical support for this program. An individual's consent under section 59 would need to be obtained or have previously been obtained before the disclosure of that individual's diagnostic, treatment and care information to the breast cancer screening database, using an automated computer network, could occur.

Another example would be disclosure of an individual's diagnostic, treatment and care information, including drug information, to alberta we//net's proposed Pharmaceutical Information Network (PIN). Doctors, pharmacies, pharmacists and health facilities will be able to access an individual's drug information that is stored in the database using the PIN.

Consent given under this section is consent to the form that the disclosure of individually identifying diagnostic, treatment and care information will take. It is not the same as consent for the disclosure of individually identifying health information under **section 34**. The consents under **section 34** and **section 59** requires separate, specific consents.

An individual may revoke his or her consent at any time **(section 59(2)(d))**. Consent, or revocation of consent, must be in writing or in valid electronic form **(section 59(4))**.

Consent must indicate that the individual has been made aware of the reason for disclosure by electronic means and the risks and benefits to the individual of consenting or refusing to consent **(section 59(2)(b))**.

Once consent is provided, it authorizes all custodians to disclose that individual's information by electronic means for all authorized purposes listed in **section 27**, subject to the rules regarding disclosure of the least amount of information, at the highest degree of anonymity and on a need to know basis.

The requirement for consent in **section 59** is intended to provide individuals with a level of control over the dissemination of their health information over computer networks.

Consent must either be given in writing or provided electronically. An **"electronic consent"** means the granting of an authority that is provided electronically. Under **section 5(2) of the Regulation**, an electronic consent or revocation of an electronic consent is valid only if the level of authentication is sufficient to identify the individual who is granting or revoking the consent.

Although written consent for disclosure through electronic means could be entered and stored on an electronic system, this is not what is meant by "electronic consent" for the purposes of **section 59(2)**.

The requirements for electronic or written consent for the purpose of **section 59** are found in **sections 59(2)-59(6)**.

A separate consent is required and must include:

- an authorization for any custodian to disclose individually identifying diagnostic, treatment and care information about the individual by electronic means for all of the purposes listed in **section 27**;
- an acknowledgment that the individual providing the consent has been made aware of the reasons for disclosure by electronic means and the risks and benefits to the individual of consenting or refusing to consent;
- the date the consent is effective; and
- a statement that the consent may be revoked at any time by the individual providing it.

See the Section 59 Consent Form in Appendix 1 of this Publication.

In addition to the above requirements:

- a revocation of a consent must be provided in writing or electronically **(section 59(4))**;
- a written consent must be signed by the person providing it **(section 59(5))**; and
- a consent or revocation of consent that is provided electronically is valid only if it complies with the requirements set out in the regulations **(section 59(6))**.

Section 59 envisions individuals giving one consent to allow their individually identifying diagnostic, treatment and care information to be disclosed through electronic means for all of the purposes outlined in **section 27**. This would include disclosure for:

- the provision of health services;
- determining or verifying eligibility to receive a health service;
- conducting investigations, discipline proceedings, practice reviews or inspections relating to the members of a health profession or health discipline;
- conducting research approved by an ethics committee;
- providing for health services provider education;
- carrying out any purpose authorized by an enactment of Alberta or Canada;
- internal management purposes; and
- for the Minister, the department, regional health authorities, the Alberta Mental Health Board and the Alberta Cancer Board, planning and resource allocation; health system management; public health surveillance; and health policy development.

An individual who consents **(under section 59)** to the disclosure of his or her diagnostic, treatment and care information has to be told that their consent **(to the means of disclosure)** can be relied upon by other custodians for any of the purposes authorized under **section 27**.

A custodian may obtain consent directly from the individual or may rely on consent previously obtained by that custodian or by another custodian. Once an individual has been asked for his or her consent, a "yes' or "no" response will be entered by the custodian into a consent registry, which stores the information. All custodians have access and update capabilities to the consent registry.

An information package on **section 59** and the associated consent registry is available from the department. The consent form will be included in the package.

The absence of consent is interpreted as the absence of authorization. Where the individual has not indicated any consent to disclosure by electronic means, a custodian cannot assume consent to this form of disclosure.

Individuals must not be penalized for refusing to consent to this form of disclosure by denying them the service for which the health information was originally collected.

Consent may be given by representatives acting on behalf of an individual in accordance with the conditions set out in **section 104(1)**.

The duties under **sections 57** (to disclose at the highest level of anonymity), **58** (to disclose the least amount of information) **and 60** (to protect the confidentiality of health information) also apply to health information disclosed by electronic means.

5.2.4 DUTY TO PROTECT HEALTH INFORMATION

Custodians are the trusted "gatekeepers" of health information. **Section 60** requires custodians to protect the privacy of individuals who are the subject of health information and the confidentiality of the health information that is in their custody or under their control. This duty to protect covers health information that is transmitted or transported to other custodians or to others outside the "controlled arena", including persons outside Alberta.

All of the rules regarding protection of health information in **section 60** of the *Act* and in **section 8** of the Health Information Regulation apply to health information in any form, format or information system. The rules apply whether the information system is paper-base, electronic or a combined system.

"Privacy" is the "general right of the individual to be left alone, to be free from interference, from surveillance and from intrusions."[1] In the context of health information protection, it is the right of an individual to be able to control access to as well as the collection, use and disclosure of his or her information.

"Confidentiality" implies a trust relationship between the person supplying information and the individual or organization collecting it. The relationship is built on the assurance that the information will only be used by or disclosed to authorized persons or to others with the individual's permission. Protecting the confidentiality of health information implies that individually identifying health information is concealed from all but authorized parties.

What Must Custodians Do to Protect Health Information?

- Under **section 60(1)(a),** custodians must take reasonable steps, in accordance with the requirements in the regulations (**section 8** of the Health Information Regulation), to maintain administrative, technical and physical safeguards to ensure the protection of health information in their custody or under their control.

  "Taking reasonable steps" means complying with the general and specific obligations and standards for health information security set out in **section 8** of the Health Information Regulation.

  "Administrative, technical and physical safeguards " generally include administrative procedures, physical standards and technical security services and mechanisms.

---

[1] Samuel Warren and Louis Brandeis, *"The Right to Privacy"*, 4 Harvard Law Review 193, 205.

- Under **section 60(1)(b)**, custodians must protect the privacy of individuals who are the subject of health information and the confidentiality of health information that is to be stored or used in a jurisdiction outside Alberta or that is to be disclosed by the custodian to a person in a jurisdiction outside Alberta.

- Under **section 60(1)(c)**, custodians must protect the health information in their custody or under their control against any reasonably anticipated:
  - threat or hazard to the security or integrity of the health information or of loss of the health information, or
  - unauthorized use, disclosure or modification of the health information or unauthorized access to the health information.

"Threat" means a sign or cause of possible harm.

"Hazard" means a risk, peril or danger.

"Security" means a condition of safety or freedom from fear or danger. In the context of health information, it refers to the physical, technological or administrative arrangements that persons or organizations use to prevent individually identifying health information from being altered, lost or disclosed without authority.

"Integrity" refers to the condition of information being whole or complete; not modified, deleted or corrupted.

"Unauthorized access" occurs when affiliates have access to health information that they do not need to see or handle in the course of their duties. It also refers to situations where members of the public gain access to an individual's health information through accidental disclosure or surreptitious means.

An example of accidental disclosure would be laboratory reports sent to the wrong facsimile number.

"Unauthorized collection" occurs when individually identifying health information is collected, acquired, received or obtained by any means for purposes that are not allowed under **section 20.** That section authorizes collection if it is expressly authorized by an act or regulation of Alberta or Canada or if the information relates directly to and is necessary for the custodian to carry out a purpose authorized under **section 27**.

(See Chapter 6 of this Publication).

"Unauthorized use" refers to the use of health information for a purpose that is not authorized under **section 27.**

(See Chapter 7 of this Publication).

"Unauthorized disclosure" refers to the act of revealing, showing, providing copies, selling, giving, or relaying the content of health information in ways that are not permitted under **sections 35 to 40, 46, 47 or 53.**

Health information may be at risk of unauthorized disclosure if the disposition of records containing health information is not monitored or controlled properly. **(See section 60(2) below and chapter 8 of this Publication)**.

"Unauthorized modification" may occur unintentionally or intentionally, through malicious code, forgery or the wrongful addition of information to a record containing health information.

- Under **section 60(1)(d)**, custodians must ensure that their employees, affiliates and information managers, (contracted to store health information or provide information management and technology services), comply with this section and with the *Act*.
- Under **section 60(2)**, custodians must maintain appropriate safeguards for the proper disposal of records to prevent any reasonably anticipated unauthorized use or disclosure of the health information or unauthorized access to the health information following its disposal.

  (See section 11.2.4 – Scheduling and Disposition of Recorded Health Information in Chapter 11 of this Publication).

  Examples of improper disposal of health information that could result in unauthorized access, use or disclosure of the information are: the shredding of health information with no authority to do so, the discarding of records containing health information in a garbage container or recycle bin, or the sale of a computer without ensuring that health information is completely and permanently removed from the hard drive.

  Destruction of health information to prevent access by the individuals who are the subject of the information is also an unauthorized disposal of the information.

What are the Reasonable Steps for Protection of Health Information that are Required by the Health Information Regulation?

- Under **section 8(1)** of the Regulation, custodians must identify and maintain a written record of all administrative, technical, and physical safeguards in respect of health information.

  This step usually begins with the establishment of an organization-wide written policy and procedures on health information security and includes an inventory of the safeguards respecting health information that will be maintained by the custodian and its affiliates.

  (See section 11.3.4 in Chapter 11 of this Publication for information on Developing a Security Policy).

- Under **section 8(2)** of the Regulation, custodians must designate an affiliate with overall responsibility for the security and protection of health information in their custody or under their control.

  This step has more relevance for larger custodians where an affiliate would be designated as having responsibility for developing, implementing, maintaining, coordinating and monitoring an information security program consistent with the requirements of the *Health Information Act* and the Regulation as well as any information security policies and procedures of the custodian. However, for single site or smaller custodians, either the custodian him/herself or an affiliate would have to take or be given this responsibility.

- Under **section 8(3)** of the Regulation, custodians must periodically assess their administrative, technical and physical safeguards in respect of:
    - the confidentiality of health information in its custody or under its control and the privacy of the individuals who are the subjects of that information;
    - any reasonably anticipated threat or hazard to the security or integrity of the health information or to the loss of the health information; and
    - any unauthorized use, disclosure or modification of the health information or unauthorized access to the health information.

To carry out this step:

- custodians should use a threat and risk assessment to determine the level of sensitivity of health information and the potential threats and risks to its security.

  "Threat and Risk Assessment" refers to the process of determining what harm or whom to protect against and then assessing whether existing or proposed security measures are satisfactory and determining vulnerabilities.

  (See section 11.3.3 in Chapter 11 of this Publication for information on conducting a Threat and Risk Assessment).

- once a Threat and Risk Assessment has been completed, custodians should take steps over time, and within available resources, to develop or adopt, implement or maintain the administrative, technical and physical safeguards necessary to protect health information in their custody or under their control.
- custodians should then periodically review the level of information security, the risks to security and the administrative, technical and physical safeguards they have put in place to protect the health information in their custody or under their control.

Depending upon the type and level of threats and risks to health information in the custody or under the control of a custodian, the following administrative, physical and technical safeguards may be used:

Administrative Safeguards

- Access to health information and access to any place or system where health information is kept must be restricted to individuals who are authorized to use, modify, transform or disclose health information to perform their assigned duties. Employees and other information users must be authorized to access, maintain, change, use or distribute information. Authorization for each information user should be based on the 'need to know' of that individual.

- Security checks may need to be employed to ensure that individuals in key employee positions are screened. This includes background checks and taking oaths of confidentiality, where necessary.

- All systems programmers, network/LAN technical staff, ID administrators, file and mailroom staff have privileged access to the work environment and have to be "trusted". Screening of personnel should be done on a regular basis, and criminal record checks may be appropriate and required in some cases.

For example, under the *Protection of Persons in Care Act,* "agencies" like hospitals and nursing homes must require every successful applicant for employment and every new volunteer to provide a criminal records check.

- Information access privileges should be reviewed, modified or revoked as necessary when:
    - an employee is transferred by appointment, assignment or secondment;
    - an employee commences an extended period of absence, including maternity, medical, military or community service;
    - access privileges have not been exercised for a period of time; or
    - the employment or contract of the individual has been terminated. Upon termination:
        - the individual should be debriefed with respect to ongoing responsibilities for the confidentiality of custodian information;
        - access privileges (system passwords, user ID's, combinations, etc.) to systems, restricted access zones, and IT facilities should be revoked; and
        - all security related items (badges, keys, documents, etc.) issued to the individual should be retrieved.

- To ensure that parties accessing information are who they say they are, the identity of any individual who accesses, uses, modifies, transforms, discloses or disposes of health information must be verified and authenticated prior to access to information being granted.

  The most common form of this safeguard in an electronic environment is the use of passwords. However, it could also include requiring proof of identification using tokens, biometrics, challenge/response scenarios, one-time passwords, digital signatures and certification authorities.

  Authentication passwords or codes must be:
    - generated, controlled and distributed in a manner which maintains the confidentiality and integrity of the code or password;
    - known only to the user of the identifier;
    - either pseudo-random in nature or verified by an automated process designed to counter triviality and repetition;
    - at least 6 characters in length;
    - one-way encrypted for storage in the computer system subject to a history check to preclude reuse;
    - prompted for manual user entry when using automatic or scripted log-on processes;
    - changed at least every 90 days; and
    - a mixture of characters, both upper and lower case, numbers, punctuation and special symbols.

- Records should be kept identifying all instances of access, use, modification, transformation, disclosure or disposal of individually identifying diagnostic, treatment and care information.

- Records must be kept of all instances of unauthorized access, use, change, deletion/disposition or disclosure of health information.

- Procedures, policies, practices and other safeguards must be implemented to minimize the risk from unauthorized access to, or unauthorized use, modification, transformation, disclosure or disposal of health information.

- Procedures, policies and practices and other safeguards must also be implemented to ensure accuracy and completeness of health information.

  The policies and procedures should be in writing, current and available to all staff. Policies, procedures and penalties should also be outlined in contracts for service providers.

  (Also refer to section 5.2.5 of this Chapter for more discussion on the duty to ensure accuracy of health information).

Physical Safeguards

- In addition to restrictions on who can access health information, access to the facility, office, information retrieval equipment and systems and information stores must be controlled to ensure that access is granted only to individuals with authorization for such access.

  These controls relate to mechanisms in a computer operating system, hardware unit, software package, file room or mailroom. This is typically a password for systems access but may include card locks, and physical security access systems such as keys, digital card keys and cipher lock barriers.

- Physical security safeguards to maintain access control can range from anti-theft systems such as bolting equipment to the floor in secure rooms, locked desks and cabinets.

- Smaller custodians with little health information in electronic form should concentrate on physical security measures (locked rooms or cabinets, adequate access controls for employees and the public and sound disposition measures for the information). Larger custodians with sensitive health information in a variety of forms and formats will have to take a wider range of security measures based upon the threat and risk analysis conducted.

- Stringent protection measures should be applied to health information with a high level of sensitivity and with a greater possibility of causing damage to an individual if it is accidentally disclosed, stolen or finds its way into unauthorized hands.

  For example, physical access control zones, locked rooms, locked filing cabinets, and personnel reliability checks may need to be employed. Information technology systems may require computer access control codes, automatic accounting of use and telecommunications security devices.

- For less sensitive health information where the risk of compromise or unauthorized access is low, a custodian may only need to put in place lower grade security measures. Examples of these would be unlocked cabinets in a controlled area that is locked at night; computers being kept behind service counters, with screens not visible to patients/clients other than the subjects of the information; and computers accessed through restricted authorization codes.

Technical Safeguards

- See also **Administrative Safeguards and Physical Safeguards** for related information about access controls and authentication passwords and codes and other forms of user verification.

- All methods of communication of health information must be secure from unauthorized access, including eavesdropping, interception and diversion.

  "All methods of communication" includes verbal communication, transmission of written documentation, telephone, cellular phone, fax, e-mail, video and audio communication or any other form of electronic communication.

  "Eavesdropping" occurs when unauthorized individuals inadvertently or through the use of deceptive techniques such as remote monitoring of conventional telephone or cellular phone conversations or voice mail, gain access to health information.

  "Interception" occurs when unauthorized individuals inadvertently or through the use of deceptive techniques gain access to health information e.g. by interrupting the flow of information over a transmission line, through the use of electronic or other means.

  "Diversion" occurs when the direction of the flow of health information is changed inadvertently or through the use of deceptive techniques so that an unauthorized recipient can gain access to it.

- Identification and authentication safeguards or the use of audit safeguards to monitor security systems and procedures may be needed. These include virus scanners, firewalls, monitoring operating system logs, software logs, version control and document disposition certification.

- Encrypted storage and transmission may also be necessary for particularly sensitive health information.

  "Encryption" refers to the technique or process of transforming information from human readable form to a meaningless form using mathematical number theory (a computational algorithm). Encryption may be used for an entire record of information, in which case it must be decrypted before it can be used at all.

  Many computer systems keep identifiable information stored in encrypted form to prevent casual access to information. Secure applications would decrypt the information prior to providing access to authorized individuals performing specific activities.

  Encryption can be used to transform a personal identifier to a unique, but anonymous identifier. Anonymous identifiers allow processing of discrete person level records to analyze information across time, data sources or geographical areas for such purposes as measuring utilization, health system performance, and health outcomes or program evaluation.

  Encryption may be hardware or software based and is usually "key" based. A Public Key Encryption system uses a publicly accessible and widely understood encoding/decoding process, a set of publicly available keys, and a secret matching set of private keys.

A **"key"** refers to a string of digits and/or characters used to encrypt or decrypt a message. The level of security often depends upon the length of the key.

- All systems hardware and software must be secure from inappropriate access, accident, misappropriation, viruses and systems failure.

- Put in place disaster recovery safeguards. These can range from the use of on-site diskettes/tapes to replication with an external system and duplication (e.g. photocopiers) on other media forms with possible off-site storage facilities.

- Other related safeguards include the use of redundant or fault tolerant equipment such as disk shadowing/mirroring, dual systems, hot backups and alternate routing. These safeguards are typically hardware based but require software/procedures to manage the environment.

- Procedures, policies and practices must be implemented to restore, replace or re-create health information that has been damaged, lost or destroyed either accidentally or deliberately.

Under **section 8(4)** of the Regulation, in order to ensure the privacy and confidentiality of health information that is to be stored or used by a person in a jurisdiction outside Alberta, or that is to be disclosed to a person in a jurisdiction outside Alberta, custodians must enter into a written agreement with the person prior to the storage, use or disclosure of the information.

The agreement must:

- provide for the custodian to retain control over the health information;
- adequately address the risks associated with the storage, use or disclosure of the health information outside Alberta;
- require the other party or parties to develop, adopt or implement and maintain the security safeguards outlined in the agreement;
- allow the custodian to monitor compliance with the terms and conditions of the agreement; and
- contain remedies to address any non-compliance with or breach of the terms and conditions of the agreement by the other party or parties.

An agreement under this section of the Regulation would be required, for example, if individually identifying health information is going to be stored in a database in another province or if the information is being processed by or disclosed to another organization or company outside Alberta. The requirement for an agreement ensures that the rules for the protection of health information inside Alberta are also applied to health information flowing to another jurisdiction, which may not have the same level (or any) data protection laws.

However, under **section 8(5)** of the Regulation, if individually identifying health information is being disclosed to a person in a jurisdiction outside Alberta solely for the purpose of providing continuing treatment and care to the individual, an agreement with the recipient is not required.

This situation could arise where an individual travels to another province and needs to have a prescription filled. The pharmacist in the other province may need a custodian (e.g. a pharmacist or physician) in Alberta to disclose the individual's drug information in order to fill the prescription.

Under **section 8(6)** of the Regulation, a custodian must ensure that all of its affiliates are aware of and adhere to all of the custodian's administrative, technical and physical safeguards in respect of health information.

Without training and awareness of the custodian's policies and procedures, no amount of technology can secure an environment. In order to conduct an on-going security awareness training program, the custodian should:

- identify the scope, goals and objectives of the program;
- identify the trainers;
- identify the target audiences;
- motivate management and employees;
- maintain the program; and
- evaluate its effectiveness.

Another way of ensuring awareness of safeguards is to provide new affiliates with copies of the custodian's information security policies and procedures; ensure that all other affiliates have continuing access to the policies and procedures through an internal website or intranet on a local area or wide area network; and attach the policies and procedures as a schedule to any contracts which require the collection, use, disclosure or protection of health information.

Under **section 8(7)** of the Regulation, custodians must establish sanctions that may be imposed against affiliates who breach, or attempt to breach, the custodian's administrative, technical and physical safeguards in respect of health information.

Sanctions can include withdrawing access privileges and disciplinary action up to and including suspension or dismissal. The sanctions for breaches of the *Act,* the Regulation or the custodian's policies and practices should also be part of the terms and conditions of contracts relating to the access to or collection, use, disclosure, storage or disposal of health information. Sanctions in the case of contractors could include termination of the contract.

Under **section 107(4),** if the contract is with an Information Manager under **section 66,** it would be an offence under the *Act* to knowingly breach any terms and conditions of the contract respecting the protection of health information.

For further information on security standards, refer to the Canadian Organization for the Advancement of Computers in Health (COACH) Guidelines (http://www.coachorg.com/publications/privacy_guidelines.htm); Government of Victoria, Australia Information Security Policy, Department of Premier and Cabinet (http://www.dpc.vic.gov.au/ocmpol/216c.htm); British Standard BS 7799: 1995 – Code of Practice for Information Security Management (http://www.bs.org.uk/disc/new/7700prod.html)

5.2.5 DUTY TO ENSURE ACCURACY OF HEALTH INFORMATION

Before using or disclosing health information that is in its custody or under its control, a custodian must make a reasonable effort to ensure that the information is accurate and complete **(section 61)**.

Part of this duty is ensuring that the source of information can be clarified and all access, disclosure and changes can be tracked and audited.

"Making a reasonable effort" means that the custodian will be thorough and comprehensive in identifying practicable means to ensure that health information is accurate and complete. As well as being a privacy requirement, verification procedures and practices to ensure accuracy and completeness are particularly good business practices for large health information systems that deliver programs.

Custodians trying to ensure accuracy and completeness may find it helpful to answer the following questions:

- Is there a system of verification for health information collected and for its entry on the system?
- Does the record indicate the last update date?
- Is a record kept of the source of the information used to make changes (e.g. paper or transaction records)?
- Is there a process in place to grant staff authorization to add, change or delete personal information from records held by the system?
- Is there a procedure for correcting or amending the information in the record?
- Does the system have the necessary audit trails to determine who may have previously relied on the incorrect information?
- Are procedures in place for disposition of personal information and are actual records retention and disposition schedules agreed upon and signed, for all the information in the system?

***BEST PRACTICE:** There should be careful verification of any health information crucial to an application, transaction or action when the information is provided. There could also be systematic processes in place for updating health information, either as a result of information provided from the individual or cross-referencing other related files providing basic identifying data.*

Other checks of accuracy might be periodic audits of files with accuracy and completeness as one of the criteria tested or establishing with the software of automated systems cross-referencing and verification checks that identify anomalies in data.

Refer to the discussion on Identification and Authentication Requirements in section 5.2.4 Duty to Protect Health Information in Chapter 5 of this Publication.

5.2.6 DUTY TO IDENTIFY RESPONSIBLE AFFILIATES

Custodians remain ultimately responsible for compliance with the *Health Information Act*. However, under **section 62,** each custodian must identify its affiliates who are responsible for ensuring compliance with the *Act*, the regulations and the policies and procedures established or adopted under

section 63. To carry out this duty, custodians must first know who their affiliates are (**see 'Who is an Affiliate' in *THINGS TO REMEMBER* at the end of Chapter 1 of this Publication**). They must then identify one or more of their affiliates who will be responsible for administering and ensuring compliance with the *Health Information Act*, the regulations under the *Act* and the custodians policies and procedures regarding the collection, use, disclosure and protection of health information.

An **"affiliate"** is defined in **section 1(1)(a)** to include an employee of a custodian; a person who performs a service for a custodian as an appointee, volunteer, student or contractor; or a health services provider who has the right to admit and treat patients at a hospital. The definition of affiliate does not include an operator under the *Ambulance Services Act* or an agent under the *Health Insurance Premiums Act.*
See section 9.3 of Chapter 9 of this Publication for more discussion regarding this duty.

5.2.7 DUTY TO ESTABLISH OR ADOPT POLICIES AND PROCEDURES

Under **section 63(1)**, custodians must establish or adopt policies and procedures that will facilitate the implementation of the *Act* and the regulations. At the request of the Minister or the department, a custodian must provide the Minister or department with a copy of such policies and procedures **(section 63(2))**.

(See section 9.4 of Chapter 9 of this Publication for more discussion regarding this duty).

5.2.8 DUTY TO PREPARE PRIVACY IMPACT ASSESSMENTS

Section 64(1) requires custodians to prepare a privacy impact assessment when the privacy of individuals may be impacted by a proposed or changed administrative practice, or a new or modified information system that collects, uses and/or discloses individually identifying health information.

The privacy impact assessment must be submitted to the Commissioner for review and comment before a custodian implements any proposed new practice or system or any proposed change to existing practices and systems relating to the collection, use or disclosure of individually identifying health information **(section 64(2))**.

What is a Privacy Impact Assessment (PIA)?

A **"privacy impact assessment" (PIA)** is a **process** that assists custodians in reviewing the impact that a new project may have on individual privacy. The process is designed to ensure that the custodian evaluates the program or scheme to ensure technical compliance with the *Health Information Act* as well as assessing the broader privacy implications for individuals.

The PIA process requires a thorough analysis of potential impacts on privacy and a consideration of measures to mitigate or eliminate any such impacts. The PIA is a due diligence exercise, in which the custodian identifies and addresses potential privacy risks that may occur in the course of its operations. While PIAs are focussed on specific projects, the process should also include an examination of organization-wide practices that could have an impact on privacy. Organizational privacy and security policies and procedures, or the lack of them, can be significant factors in the ability of the custodian to ensure that privacy protecting measures are available for specific projects.

A PIA provides documented assurance to the custodian, to the Commissioner and to the public that all privacy issues related to the initiative have been appropriately identified and addressed.

When is a Privacy Impact Assessment Needed?

Custodians undertaking the following types of initiatives will likely need to conduct a PIA under **section 64(1)** when:

- a proposed system or a proposed administrative practice will relate to the collection, storage, use, disclosure, linkage and/or matching of health information that is, or could be made to be, individually identifying;
- new data elements will be collected and added to an existing health information database or a new database is proposed;
- system access will be rolled out beyond current parameters, controls, levels or numbers of users;
- health information use will be expanded to include data linkage or matching or other purposes and uses;
- limited disclosure or reporting about selected individuals will be expanded to enable broad disclosure of information about a larger population base (or even the entire population of Alberta);
- the way in which the system is accessed, managed or secured from a technical or managerial perspective is changed significantly (including use of internet technology or outsourcing); and/or
- retention periods for the health information in the system will be changed.

In addition to the above, there are requirements for a PIA under **sections 70(2), 71(2), 72 and 46(5).** These requirements are dealt with later in this section of the Chapter.

When is a Privacy Impact Assessment Not Needed?

A PIA may not be needed when the proposed system or administrative practice relates to the collection, storage, use or disclosure exclusively of non-identifying or aggregate health information.

As information systems become more complex, the probability of having an unexpected privacy impact increases. Initiatives that appear to involve minor technical enhancements for client convenience and custodian efficiency may significantly impact individual privacy

Keeping this in mind, the following are examples of initiatives that may not require a PIA:

- minor changes to the scope of program information requirements, such as the collection of additional eligibility data as authorized by statute and reflected in revised notices or consents;
- data matching agreements where a privacy impact assessment on the data matching has already been developed;
- routine system maintenance such as minor software upgrades or patches, replacement of equipment that does not materially change information management functions or system security; or

- minor upgrades to systems which have no impact on the way in which health information is managed.

What is the Process for a Privacy Impact Assessment?

1. Management of the Process

The following are relevant considerations in managing the PIA process:

- composition of the PIA development team. Determine which affiliates can best provide the information needed. These would potentially be the Health Information Coordinator or whichever affiliate(s) has (have) been designated with this responsibility; project or program sponsors; records managers; project managers and IT/IM specialists; legal services; communications; and senior/executive management;
- identifying someone to lead the process and write the PIA. Ideally this requires someone who understands the *Health Information Act* and privacy principles and issues; has technical writing skills; has project management experience; and can reflect input from a variety of sources.

2. Timing of the Process

If the PIA is viewed as an obstacle to the initiative being launched, it has been started too late. If decisions about the initiative are not firm, resources have not been committed and questions about privacy implications cannot be answered, it is too early to start the process.

It is the view of the Office of the Information and Privacy Commissioner that a PIA is rarely ever finished. It is a dynamic document that should be updated from time to time as changes are contemplated for the program. It is expected that an organization will advise the Commissioner's Office of any changes or modifications to the program and provide documentation so that the assessment on file is always up to date.

3. Internal Approval of the PIA

The internal approval of a PIA should be based on the custodian's established internal approval process and should include approval from the members of the PIA development team.

4. Public Consultation

As part of the process, it may be appropriate to consult with stakeholders or with a larger public audience on major initiatives, or on significant overhauls of existing programs. Consultation might involve only certain affected stakeholders or broader segments of the public. Focused public discussion conducted early in the process can help program or system designers anticipate public reaction to proposals or help to eliminate options that meet with significant resistance.

The custodian should address how it intends to educate and consult with affected stakeholders respecting the proposed initiative. Alternatively, the justification for not undertaking public consultation should be set out.

5. The Role of the Office of the Information and Privacy Commissioner

The PIA must be submitted to the Office of the Information and Privacy Commissioner for review and comment before implementing the proposed new practice or system or any proposed change to existing practices and systems **(section 64(2))**.

Because the onus always remains on the custodian to ensure adequate levels of privacy protection, the Commissioner will not "approve" a PIA submitted to his office. Once satisfied that the organization has addressed the relevant considerations and is committed to the provision of the necessary level of privacy protection, the Commissioner will "accept" the PIA. The PIA cannot be used to obtain a waiver of, or relaxation from, any requirement of the *Health Information Act.*

To give the Commissioner enough time to formally review and comment on a PIA, custodians should provide the PIA to the Commissioner's office at least 45 working days before implementing the proposed new or changed practice or system.

In practice, however, the Commissioner's role starts long before the formal review. The process for interaction with the Commissioner's Office (OIPC) regarding a PIA is as follows:

- The custodian advises the OIPC in writing about the project.
- If necessary, the custodian's PIA development team meets with the OIPC staff to review the project and determine if a PIA is required. The Commissioner decides if a PIA is required.
- If no PIA is required, the process is concluded.
- If a PIA is required, the OIPC requests a PIA. If a PIA is required, it must be submitted to the Commissioner by the chief executive officer of the custodian (or equivalent) or by the custodian where that is a single practitioner.
- The PIA development team prepares the PIA by completing a PIA questionnaire, with the necessary elaboration and enclosures and submits it (from the appropriate officer) to the Commissioner.
- Questionnaire responses are reviewed by the OPIC within 30 working days and discussed with the PIA development team as required. Further information may be requested, in which cases the review period may exceed 30 working days.
- Upon final acceptance by the OIPC, the custodian receives a letter of acceptance from the Commissioner. This letter also advises of any future activity from the OIPC.
- The PIA is filed in the OIPC Library and is available for public review. (Public access to some confidential information, such as details of sensitive security measures, is sometimes restricted. Any such restrictions are limited and specific).
- The custodian provides updates to the PIA as changes to the project are implemented over time.

It is the view of the OIPC that a PIA is rarely ever finished. It is a dynamic document that should be updated from time to time as changes are contemplated for the program. It is expected that a custodian will advise the OIPC of any changes or modifications to the program and provide documentation so that the assessment on file is always up to date.

The OIPC may utilize the PIA as a starting point for any investigation into a breach of privacy.

The Office of the Information and Privacy Commissioner publishes a document on the Privacy Impact Assessment Process called "Privacy Impact Assessment: Instructions and Annotated Questionnaire". This package is available for downloading from the Commissioner's web site at http://www.oipc.ab.ca. Alternatively, custodians may e-mail a request for a PIA package to ipcab@oipc.ab.ca or telephone (780) 422-6860.

Privacy Impact Assessment Questionnaire

The PIA Questionnaire will be considered a public document by the OIPC. Any enclosures will also be considered public documents, unless they are explicitly designated as "confidential." Enclosures could include such documents as an organizational strategic or business plan addressing privacy protection or physical or information technology security plans and access control documentation. Enclosures that are designated as confidential must be accompanied by the reasons for confidentiality.

The PIA Questionnaire must be submitted to the Commissioner with a covering letter from the chief executive officer of the custodian (institutional) or from a regulated health professional who is the custodian. Otherwise, it will not receive a formal response.

How is the Questionnaire Completed?

The questionnaire is divided into the following two parts:

- Part A: Organizational Privacy Management
- Part B: Project Privacy Management

Each part contains a series of questions. The checkboxes on the questionnaire provide for summary responses to the questions and the note fields provide for elaboration of the responses, as necessary. There is also a column that can be used to cross-reference separate enclosures. The questionnaire can be completed either in paper or electronic formats.

Part A: Organizational Privacy Management

This part of the questionnaire is intended to provide background on organization or custodian-wide facets of privacy management that may affect the management of privacy issues for the specific project. If this information has been provided with a previous PIA and has not changed, it does not have to be resubmitted.

The questions for each section of Part A are:

1. Privacy Policies and Controls

- Does the custodian have an organizational strategic plan or business plan that addresses privacy protection? If so, enclose the information.

- Does a written privacy charter or policy (plan, or mission statement) exist? If so, enclose the information.

- Have privacy guidelines, including policies, been developed for various aspects of the custodian's operations? If so, enclose the information.

- Is the custodian subject to statutory provisions regarding privacy and confidentiality, other than those provided by the *Health Information Act* (and the *FOIP Act* for custodians that are also public bodies under the *FOIP Act*)? Is the legislation expressly paramount over the *Health Information Act*? Enclose the relevant statutory provisions.

- Does the custodian have policies or procedures in place to ensure that:
  - there is statutory authority to collect health information (either under the *Health Information Act* or another statute or regulation);
  - individual consent is obtained when that is required;
  - individuals are duly informed of the purpose and authority for collection of health information;
  - individuals have a right to request access to their own health information;
  - individuals have a right to request correction or amendment of their health information and annotation procedures are available when required; and
  - records are appropriately stored and managed to protect the privacy of individuals and the confidentiality of their health information?
    If so, provide the policies and procedures.

- Are privacy controls in place within the custodian that include:
  - need-to-know policies and procedures for access to and use of health information;
  - physical security and access controls;
  - IT security and access controls;
  - waste management (disposal) controls for health information;
  - records management policies and retention and disposition schedules;
  - enclose the relevant policies and procedures.

- Does the custodian have an information security plan or policy? If so, enclose it.

(See section 11.3.4 of Chapter 11 of this Publication for information on Developing a Security Policy)

2. Privacy Structure and Organization

- Has an affiliate been designated with responsibility for the security and protection of health information in the custody or under the control of the custodian? If so, identify the position.

- Does a reporting process exist to ensure that the managers of the custodian are informed of any privacy compliance issues?

- Is senior management of the custodian (if any) actively involved in the development, implementation and/or promotion of privacy measures within the custodian?

- Are affiliates provided with training related to the protection of health information?

Part B: Project Privacy Management

In this part of the questionnaire, the custodian provides information specific to the proposed project. The questions for each section of Part B are:

1. Project Description

- Has a summary of the proposed project been prepared, including a description of the needs behind the development of the project and how the proposed project will meet those needs? Enclose the summary.

- Has a listing of all health information or data elements to be collected, used or disclosed in the project been prepared? Enclose the listing.

  This section of Part B identifies and traces health information from the point of collection to the point where all copies of the information are destroyed or permanently archived. It should include the following steps:
  - group the data elements into registration information, diagnostic, treatment and care information and health services provider information;
  - identify the information source – whether the information is collected directly from each individual by the business or program area responsible for the initiative; from an internal information system within the custodian; or from an external source;
  - identify the rationale for each data element collected (e.g. needed for identification, contact, to verify eligibility, etc.);
  - indicate the degree of anonymity of the health information being collected to carry out the intended purpose(s) (e.g. aggregate, non-identifying, individually identifying);
  - if individually identifying health information is collected, explain why aggregate or non-identifying health information is not adequate for the intended purpose(s) **(section 57)**; and
  - describe the process(es) used to determine the amount of personal health information collected (e.g. the data elements and the target population) **(section 58)**.

- Have diagrams been prepared showing the flow of health information for this project? If so, provide the diagram(s).

  The information flow diagram could be a flow chart or schematic or a structured analysis of a series of progressive steps in a program, broken down according to function. The diagram should illustrate how health information is collected, how it circulates within the custodian(s) and how it is disseminated beyond the custodian(s).

- Have documents been prepared showing which persons, positions or affiliate categories will have access to which elements of health information and where copies of records accessed or used may exist? Enclose the documents.

  This will illustrate the need-to-know principle. This information may be able to be incorporated into the information flow diagram.

2. Authority for Collection, Use and Disclosure of Health Information

- The custodian needs to analyze the proposed information flows against the rules in the *Health Information Act* regarding collection, use, disclosure, protection, accuracy, retention and disposition of health information as well as the right of access and the right to request a correction or amendment to an individual's health information.

- Has the legal authority for the collection, use and disclosure of all personal information for this project been established? Enclose statutory provisions.

Collection of Health Information (Sections 19 & 20)

- Is individually identifying health information being collected?
- What is the authority for the collection? (attach statutory references, if any)
- Has only necessary health information been collected (on a need to know basis)?
- Is the information being collected at the highest level of anonymity possible and in a limited manner? **(sections 57 and 58)**
- If individually identifying diagnostic, treatment and care information is being collected from another custodian by electronic means, has that custodian obtained consent from the individual subjects for disclosure of their health information by electronic means, or ensured that consent was previously obtained? **(section 59)**

Collection of Personal Health Number (Section 21)

- What authority requires individuals to provide their personal health number (if this needs to be collected)?

Manner of Collection of Health Information (Section 22)

- Is individually identifying health information collected directly from the individuals it is about?
- How will affected individuals be notified of the legal authority for and purpose(s) for the collection as well as the contact information **(section 22(3))**?
- If individually identifying health information is being collected indirectly, what is the authority for the indirect collection and what is the source?
- Is the information flowing from another custodian or another system?
- If there is a linkage to another database is it on a one time only or on an on-going basis?

Use of Health Information (Sections 27 - 30)

- Is individually identifying health information being used?
- Have all the anticipated uses been identified and are they authorized uses under **section 27**?
- If the personal health number has been collected, is it only being used for the purpose for which it was collected?
- Is the health information being used at the highest level of anonymity possible and in a limited manner? **(sections 57 and 58)**
- Is the health information only being used by those who have a need to know?
- Has a reasonable effort been made to ensure that the information being used is accurate and complete **(section 61)**?

Disclosure of Health Information (Sections 34 – 45)

- Is individually identifying health information being disclosed?
- Will this be an ad hoc or one-time disclosure of information or will the disclosure be on a planned (or regular) basis?
- Who will the records containing this information be disclosed to or who will have access to them? Will they have full access or limited access? (e.g. different levels of access to portions of a database or data warehouse)
- Is a new record containing health information created as a result of the disclosure?

- Have all the anticipated disclosures of individually identifying diagnostic, treatment and care information been identified and authorized under **sections 34, 35 or 39**?
- Is information on disclosures of individually identifying diagnostic, treatment and care information maintained **(section 41)**?
- Have all the anticipated disclosures of registration information been identified and authorized under **section 36**?
- Have all the anticipated disclosures of health services provider information been identified and authorized under **section 37**?
- If there is an anticipated disclosure of individually identifying health information to the Minister, is there authority to disclose under **section 40**?
- How will the recipient of individually identifying diagnostic, treatment and care information be notified of the purpose of the disclosure and the authority under which the disclosure is made if the disclosure is to a person or organization other than those in **section 42(2)**?
- How will the custodian disclosing the health information ensure that the person to whom the disclosure is made is the person intended and authorized to receive the information **(section 45)**?
- Is the health information being disclosed at the highest degree of anonymity possible and in a limited manner **(sections 57 and 58)**?
- Is the health information only being disclosed to those who have a need to know?

Disclosure to Minister or Department for Health System Purposes (Section 46)

- If individually identifying health information is being disclosed by a custodian to the Minister or the Department, is there authority to disclose under **section 46(1)**?
- Is there authority for the Minister or Department to disclose this information to another custodian **(section 46(4))**?
- If the information to be disclosed to the Minister or Department relates to a health service provided by the other custodian under **section 46(1)(b),** has the required PIA been completed and have the comments of the Commissioner been considered **(section 46(5))**?

Disclosure to Other Custodians for Health System Purposes (Section 47)

- If individually identifying health information is being disclosed to certain custodians under **section 47,** is there authority for that disclosure under **section 47**?
- Is there authority for the custodian receiving the information to disclose this information to another custodian, to the Minister or to the Department under **section 47(5)**?

Disclosure for Research Purposes (Sections 48 – 56)

- If the disclosure is for research purposes, have the requirements in **sections 49-56** been complied with?
- Has a proposal from a researcher been reviewed by an ethics committee under **sections 49 and 50**?
- Has the researcher applied to the custodian for disclosure of the health information to be used in the research and provided the response of the ethics committee to that custodian **(section 52)**?
- Has the researcher entered into an agreement with the custodian in accordance with **section 54**?

- If there is a need to collect additional health information, has the custodian or affiliate obtained consents from the individuals to be contacted by the researcher **(section 55)**?
- If the research involves data matching of individually identifying diagnostic, treatment and care information, have the provisions in **sections 48-56** been complied with **(section 72)**?

  Note that the definition of **"health information" in Division 3 of the *Act* (disclosure for research purposes)** refers to individually identifying diagnostic, treatment and care information or individually identifying registration information, or both. Even though an ethics committee review may have been conducted under **section 50,** the disclosure of individually identifying health information would still require a PIA to be conducted. However, the portions of the assessment done by the ethics committee related to security safeguards could be used in the PIA.

Disclosure By Electronic Means (Section 59)

- If individually identifying diagnostic, treatment and care information is being disclosed electronically, have the individuals who are the subjects of the information consented to disclosure by electronic means in accordance with **section 59**?

Duty to Ensure Accuracy of Health Information (Section 61)

- Has a reasonable effort been made to ensure that the information being disclosed is accurate and complete **(section 61)**?
- Is there a system of verification for health information collected and for its entry on the system?
- Does the record indicate the last update date?
- Is a record kept of the source of the information used to make changes (e.g. paper or transaction records)?
- Is there a process in place to grant staff authorization to add, change or delete personal information from records held by the system?
- Is there a procedure for correcting or amending the information in the record?
- Does the system have the necessary audit trails to determine who may have previously relied on the incorrect information?

Duty to Protect Health Information (Section 60)

- Have reasonable steps been taken, in accordance with the regulations and with **section 60,** to maintain administrative, technical and physical safeguards to ensure the protection of health information?
- If health information is going to be stored or used in a jurisdiction outside Alberta or disclosed to a person in a jurisdiction outside Alberta, how will the confidentiality of that information and the privacy of individuals who are the subject of that information be protected?
- Is there a responsible official who has the security authority for the system or administrative practice?
- Has there been an expert review of all the risks and vulnerabilities as well as the reasonableness of the proposed safeguards to protect health information against unauthorized or improper access, collection, use, disclosure and disposal of the information?

- Are there documented procedures for collecting, processing, accessing, transmitting, storing and disposing of the health information?
- Have affiliates been trained in requirements for protecting health information and are they aware of policies regarding breaches of security or confidentiality and sanctions for unauthorized collection, access, use or disclosure of health information?
- Are there controls in place over the process of who receives authority to add, change or delete health information from records?
- Is the system designed so that access and changes to health information can be audited by date and user identification?
- Are access rights only provided to users who actually require access for the stated purposes of collection?
- Is user access to health information limited to only that required to discharge the assigned functions?
- Are the security safeguards commensurate with the sensitivity of the health information and its vulnerability to compromise?
- Are there appropriate physical security measures such as security access zones, locked rooms, storage cabinets; controlled access to computer terminals and faxes to prevent random access; checkout and secure transmission procedures for files?
- Are there contingency plans and mechanisms in place to identify security breaches or disclosures of health information in error?
- If health information will be used in the electronic delivery of services, have technological tools and system design techniques been considered which may enhance both privacy and security (e.g. encryption, digital signatures, other transformation technologies)? **(see also section 5.3.1 in this Chapter regarding the Power to Transform Health Information).**
- Are procedures in place for disposition of personal information and are actual records retention and disposition schedules agreed upon and signed for all the information in the system? **(Note that the regulation regarding retention, disposition and archival storage of health information is under development but other statutes, regulations and policies may currently govern retention periods).**

Right of Individual to Access Health Information (Section 7)

- Are procedures in place to ensure that an individual can review a record containing that individual's health information?
- When an individual challenges the denial of access to a record, is he or she provided with information about the right to request a review of this decision?

Right of Individual to Request Correction or Amendment of Health Information (Section 13)

- Will the system incorporate a process to accommodate requests for correction or amendment under **section 13**?
- Does the system include disclosure or audit trails or logs to determine who may have relied on incorrect information?
- When an individual challenges the accuracy of a record, is he or provided with information about the right to request a review of the decision or the right to submit a statement of disagreement **(section 14)**?

3. Privacy Risk Assessment

The custodian identifies the potential privacy risks of the project and shows whether those risks have been successfully addressed through system design or policy measures or through other proposed options for mitigation. The residual risks that cannot be addressed through the proposed options should also be identified. Where possible, the likely implications of those risks in terms of public reaction and project success should be analyzed.

- Will personal information collected or used in the project be disclosed to any persons who are not affiliates?
- Will this project involve the collection, use or disclosure of any health information beyond Alberta's borders? Provide details (see Duty to Protect above).
- Has the project's potential risks to privacy been assessed? Provide details in an enclosure. This involves identifying, from the perspective of the individuals who are the subjects of the health information, how the project may affect their privacy interests.
- If potential risks to privacy have been identified, have means to avert or mitigate those risks been incorporated into the project design?
- Have key stakeholders been provided with an opportunity to comment on the privacy protection implications of the project? Provide the results of consultation, if any.
- Are project affiliates trained in the requirements for projecting health information and aware of the relevant policies regarding breaches of security or confidentiality? Describe the training plan.
- Are personal identifiers used to link or cross-reference multiple databases?

  The response to this question should explain the need for such linkage and the effect on the project if such linkages were not possible **(see also PIAs Before Data Matching below).**

4. Privacy Controls and Security

- Have security procedures for the collection, transmission, storage and disposal of personal information, and access to it, been documented? Enclose procedures (see Duty to Protect above).
- Are privacy controls in place for the project? Enclose details.

5. Audit and Enforcement

- Have arrangements been made for audit, compliance and enforcement mechanisms for the project, including fulfillment of the commitments made in the PIA?

  The custodian needs to show how it will demonstrate its compliance with the *Health Information Act* and its own commitments.

  Include information about how often an audit will be conducted, who is responsible for the audit, and how any identified privacy issues will be addressed.

Privacy Impact Assessments Before Data Matching

Under **section 69**, a custodian may perform data matching using information that is in its custody or under its control. If the data matching is being conducted for an authorized purpose (under **section 27(1) or (2)**) and does not relate to a new or modified administrative practice or information system that may affect the privacy of the individual who is the subject of the information, a PIA under **section 64** would not be required.

Under **section 70(2)**, before a custodian performs data matching by combining information in its custody or under its control with information in the custody or under the control of another custodian a PIA must be prepared by the custodian in whose custody and control the information created by the data matching will be stored. The PIA must be submitted to the Commissioner for review and comment.

The PIA must:

- describe how the information to be used in the data matching is to be collected; and
- set out how the information that is created through data matching is to be used or disclosed.

Under **section 71(2)**, before a custodian performs data matching by combining information in its custody or under its control with information that is in the custody or under the control of a non-custodian, a PIA must be prepared by the custodian and submitted to the Commissioner for review and comment.

The PIA must:

- describe how the information to be used in the data matching is to be collected; and
- set out how the information that is created through data matching is to be used or disclosed.

Under **section 72**, before data matching is performed for the purpose of conducting research using individually identifying diagnostic, treatment and care information, in addition to a PIA, **sections 48-56** must also be complied with.

For more discussion of Data Matching Rules, refer to section 5.4 in this Chapter. For more discussion of Disclosure for Research Purposes, refer to section 8.15 of Chapter 8 of this Publication.

Privacy Impact Assessments Before Disclosure of Health Information to Minister and Department (Section 46)

Under section 46(5), if the Minister or Department of Alberta Health and Wellness request(s) another custodian to disclose individually identifying health information relating to a health service provided by the other custodian that is:

- fully or partially paid for by the Department; or
- provided using financial, physical or human resources provided, administered or paid for by the Department;

The Department must prepare a PIA and submit it to the Commissioner for review and comment. The PIA must describe how disclosure of the health information may affect the privacy of the individual who is the subject of the information. The Department must consider the comments of the Commissioner, if any, made in response to the PIA before disclosing the health information to the following custodians:

- a provincial health board (e.g. Alberta Mental Health Board) as defined in **section 1(1)(iii)**;
- a regional health authority as defined in **section 1(1)(iv)**; or
- the Alberta Cancer Board **(section 1(1)(vii)**.

5.3 POWERS OF CUSTODIANS

The powers of custodians are set out in **Part 6 of the *Act* (Powers and Duties of Custodians Relating to Health Information).** They include the power to transform individually identifying health information to create non-identifying health information; the power to enter agreements with information managers; and the power to charge fees for producing a copy of an individual's health information.

These powers are related to two of the fundamental purposes of the *Health Information Act*: establishing strong and effective mechanisms to protect the privacy and confidentiality of an individual's health information **(section 2(a))** and providing individuals with a right of access to health information about themselves **(section 2(d))**.

5.3.1 POWER TO TRANSFORM HEALTH INFORMATION

Collecting health information in identifying form helps ensure that information collected over time relates to the same individual. However, if the end use of the information does not require knowledge of the identity of the individual, the highest degree of anonymity principle in the *Act* **(section 57(2))** places a duty on custodians to change individually identifying health information into non-identifying information.

The collection, use and disclosure of health information in electronic form and the use of information system tools allows custodians to transform individually identifying information into non-identifying or anonymous information as a means of protecting the privacy of individuals.

Under **section 65,** a custodian may, in accordance with the regulations, strip, encode or otherwise transform individually identifying health information to create non-identifying health information. **(Note that no regulations have been developed under the *Act* as yet)**. **Section 66** enables custodians to enter into an agreement with an information manager to perform the transformation function.

Definition of Terms

"Anonymous information" refers to either aggregate or individual anonymous information.

"Non-identifying health information" is defined in **section 1(1)(r)** to mean that the identity of the individual who is the subject of the information cannot be readily ascertained from the information.

"Individually identifying health information" is defined in **section 1(1)(p)** to mean that the identity of the individual who is the subject of the information can be readily ascertained form the information.

"Anonymity" refers to the characteristic of being non-identifying. That is, the identity of the individual to whom it pertains cannot be readily ascertained.

"Anonymity transformation" refers to the process of taking individually identifying health information and rendering it non-identifying.

"Stripping" refers to the technique or process of removing names and personal identifiers from records that were identifiable. The resulting records are essentially anonymous when viewed in isolation from other contextual information. However, information representing distinguishing characteristics may be sufficient to re-identify the individual when compared with other information sources which have both the distinguishing characteristics and the names.

"Encrypting" refers to the technique or process of transforming information from human readable form to a meaningless form using a computational algorithm (recipe). Encryption can be used for an entire record of information, in which case it must be decrypted before it can be used at all. Secure applications decrypt the information prior to providing access to authorized individuals performing specific activities.

Encryption can be used to transform a personal identifier to a unique, but anonymous identifier. Anonymous identifiers allow processing of discrete person level records to analyze information across time, data sources or geographical areas for such purposes as measuring utilization, health system performance, and health outcomes or program evaluation.

"Re-coding" refers to the technique or process of transforming a very specific value for a data element to one which is meaningful but less precise. An example would be to transform a birth date to an age at a point in time. Re-coding is useful when the purpose for which information is desired does not require the same degree of specificity as the purpose for which the information was first recorded.

"Abstracting" refers to the technique or process of transforming information by selecting only the relevant aspects from a complete set of information. This process is useful when the purpose for which the information is desired does not require the full set available and meets the principle of minimum amount of information used for each specific purpose.

"Aggregating" refers to the technique or process of transforming information about individuals into information about groups of individuals with common characteristics. An example would be statistical tables that count the number of individuals falling into specific groups. However, if there are only a small number of individuals within a certain category, they may be able to be identified by context.

"Deriving" refers to the technique or process of transforming specific elements of information into a new piece of information through a mathematical calculation. The derived element of information may be more meaningful to a particular purpose and also less likely to reveal identity than the specific elements from which it was derived. An example would be the length of stay in a facility that can be derived from the difference between the date of admission and the date of discharge. Both the admission date and the discharge date can be used to identify a record of an individual even though the identity had been encrypted or stripped if compared to a source of information which contained both dates and names.

"Readily ascertained" in the context of **section 57**, means that the identity of an individual (e.g. the individual's name or other identifiers or distinguishing characteristics associated with an individual) can be determined or deduced without having to apply a sophisticated technical method or process, or without having the particular technical expertise to do so.

The identity of an individual can said to be "readily ascertained" if:

- it can be determined by combining available data or information within the same or in several different records held by the same custodian;
- it can be determined by comparing information representing distinguishing characteristics with other information sources having both the distinguishing characteristics and the names or other identifiers of individuals; and
- if only readily available or conventional computer hardware, software and technical expertise is used.

Anonymity transformation techniques can be used in combination to achieve the greatest degree of anonymity with the least amount of information to meet a specific purpose. The context of use must be taken into consideration when selecting which transformation techniques to use. Information intended for public disclosure should be carefully examined after transformation to ensure that identity cannot be inferred from available context.
In order to comply with **section 65**, custodians should:

- provide non-identifying health information (either a view or a unique data set) to affiliates who have no requirement to access or use individually identifying information to meet their responsibilities;
    - although a custodian may collect health information in individually identifying form, if an affiliate does not need to access or use individually identifying information to meet his/her/its responsibilities, the custodian must transform the identifying information into non-identifying form prior to use by that affiliate; and
    - for affiliates with have multi-task roles, some of their roles may require access to or use of individually identifying information. However, the need to know principle would continue to apply to these affiliates so that they would only access individually identifying information when that was necessary to carry out a particular role.

***BEST PRACTICE:** Many purposes can be supported with the same anonymous information. Custodians could apply stripping and encryption techniques on the obvious individually identifying information but leave the other information in its originally collected form. The anonymous multi-purpose information could be stored separately from the information in identifiable form.*

Affiliates accessing anonymous information must be aware of the degree of anonymity provided by different techniques and should ensure that the principles of limited information at the highest degree of anonymity are consistently applied. Further transformation techniques may need to be applied to produce information appropriate for a specific purpose.

- disclose only non-identifying health information to other custodians who have no requirement to collect or use individually identifying information to meet their responsibilities;
    - if another custodian does not need individually identifying information to carry out its purpose, the disclosing custodian should transform the information into non-identifying information before disclosing it for the other custodian's intended use.

BEST PRACTICE: *If multiple custodians are collecting the same information from one custodian and only need non-identifying information, the coordination of anonymity transformation might require the services of an information manager to produce comprehensive non-identifying information (****under section 66****). If this is not the case, the techniques used for anonymity transformation would be similar to those employed by the collecting custodian for its own use.*

Custodians should be able to demonstrate to the Commissioner upon review that necessity for the intended purpose was considered and that non-identifying information was disclosed.

- disclose only non-identifying health information to non-custodians who have no requirement or authority to collect or use health information in individually identifying form;
    - the transformation techniques used prior to disclosing health information to a non-custodian should be chosen to produce the required degree of specificity of both information content and amount of information to meet the purpose while still reducing the risk of revealing identity; and
    - when a custodian discloses a record set containing non-identifying information to a non-custodian, the custodian must tell the recipient (in accordance with **section 32(2)**) that the Commissioner has to be notified if the non-custodian intends to use the information for data matching. The Commissioner has to be notified of this intent before the data matching is performed.

BEST PRACTICE: *The more a recipient knows about a group of individuals, the greater is the risk that identity can be inferred from non-identifying information about that same group of individuals. Additional transformation techniques such as sampling, random rounding for aggregate measures representing small populations, or adjusting the specificity of information disclosed about anonymous individuals help to minimize the risk.*

Anonymity Transformation Performed by an Information Manager

When non-identifying information is going to be used to compile population level information, the information needs to be produced in a comprehensive and coordinated manner. To accomplish this, individually identifying health information could be disclosed to an information manager to apply a common anonymity transformation technique. The resulting non-identifying records can then be analyzed across custodians to produce useful longitudinal results leading to program evaluation, health outcome measures or other statistics impossible to produce with fragmented information.

Different encryption algorithms can be used to produce population level information for different purposes. Purpose specific encryption enables coordinated, comprehensive information to be produced while not violating the principle of collecting and using the minimum amount of information needed to meet the purpose.

BEST PRACTICES: *If Information Managers are used to transform individually identifying health information into non-identifying information, the requirements of* ***section 66*** *must be followed. The custodian* *must enter into an agreement with the Information Manager, in accordance with the regulations. The transformations must be done in such a way that accumulation of anonymous information does not risk revealing identity.*

The Minister, the department, regional health authorities, the Alberta Mental Health Board, the Alberta Cancer Board will have to develop appropriate processes and policies to manage transformation, access to and disclosure of non-identifying information.

When developing new or significantly modifying automated information systems, a privacy impact assessment must be conducted. This could identify opportunities to use anonymity transformation techniques. The assessment should also identify whether anonymity transformation must be coordinated with other custodians to meet the specified purposes.

5.3.2 POWER TO ENTER AGREEMENT WITH INFORMATION MANAGER

Custodians have the power, under **section 66(2)**, to enter agreements with Information Managers, in accordance with the regulations **(note there is currently no regulation related to this power)**, to perform the following functions and to provide the following information technology services:

- process, store, retrieve or dispose of health information;
- in accordance with the regulations, strip, encode or otherwise transform, individually identifying health information to create non-identifying health information; and
- provide information management or information technology services.

"Information Manager" means a person or body that performs one or more of the functions or provides one or more of the services above (as described in **section 66(1)**). The Canadian Institute for Health Information (CIHI) and alberta we//net would be examples of information managers. A company that provides a billing service to physicians in a clinic would also be an information manager although the information would probably be limited to billing information.

Information Managers like other affiliates, fall within the controlled arena for sharing individually identifying health information. Because of the special nature of the information management services that they provide and the associated security requirements, the agreements with information managers will have special requirements. The Minister may, in the future, put these requirements into a regulation authorized by **section 108(2)(b)**.

See section 5.3.1 of this Chapter for a discussion about "transforming information" and definitions for "stripping" and "encoding".

After a custodian has entered into an agreement **under section 66(2)**, the custodian may disclose health information to the Information Manager without the consent of the individuals who are the subjects of the information for the purposes authorized by the agreement **(section 66(3))**.

An Information Manager may use the information disclosed by the custodian **(under section 66(3))** only for the purposes authorized by the agreement **(section 66(4))**. The Information Manager must comply with the *Act* and the regulations as well as the agreement entered into with the custodian **(section 66(5))**. It is an offence under the *Act* for an Information Manager to knowingly breach the terms and conditions of such an agreement **(section 107(4))**.

An Information Manager may disclose health information to the custodian that provided the information to the Information Manager. An Information Manager may disclose health information to a custodian other than the custodian that provided the information to the Information Manager only if the Information Manager has been appointed as an affiliate of that (or those) other custodian(s) and only as authorized by the custodian, according to the disclosure rules and processes outlined in the *Act* and the agreement.

However, it is important for custodians to understand that they continue to be responsible for complying with the *Act* and the regulations respecting the information that they have disclosed to the Information Manager **(section 66(6))**. This includes their responsibilities under **section 58** (collecting, using and disclosing the least amount of information needed for the intended purpose). In order to satisfy these responsibilities under that section, a custodian must:

- minimize the health information that the custodian contributes to the database;
- implement security precautions to restrict access to information in the database by participating custodians or structure the database so that participating custodians do not have direct access to it;
- obtain the consent of the individuals who are the subjects of the health information in the database; and
- obtain the advice and recommendations of the Information and Privacy Commissioner before the database is operational.

BEST PRACTICE: *Agreements with Information Managers and the related policies and procedures of the custodian need to allow the custodian to monitor and periodically audit the performance of the Information Manager under the agreement to ensure compliance with these requirements. There should also be provision for remedies such as cancellation of the agreement in the event that the Information Manager fails to meet its terms and conditions or fails to comply with the Act or the regulations.*

See Appendix 4 of this Publication for the Components of an Agreement to Disclose Health Information to an Information Manager.

Canadian Institute for Health Information

The Canadian Institute of Health Information (CIHI) is a national, federally chartered, not-for-profit organization responsible for developing and maintaining a comprehensive health information system for Canada. CIHI works toward improving the health of Canadians and the health system by providing quality and timely health information to: advance Canada's health policies, improve the health of the population, strengthen the health system, and assist leaders in the health sector make informed decisions. CIHI does not provide health services, but supports the health system by producing health information for management decision making.

Under the *Health Information Act*, CIHI is an Information Manager for the Minister and health authorities. The responsibilities and obligations of CIHI as an Information Manager are outlined in the master agreement between CIHI and the Minister.

Health information is currently sent from Alberta to CIHI directly from health authorities or indirectly from the health authorities via the department. CIHI edits the data and uses it to populate its databases. The data collected from Alberta and maintained in the CIHI databases is used by CIHI for the purpose of research and analysis of health utilization and management. The use of this data is consistent with the uses identified in the agreement. CIHI has policies respecting disclosure of data and does not provide access to Alberta identifiable data without the approval of the Minister.

In compliance with the *Health Information Act* and in accordance with the terms and conditions of its agreement with the Minister, CIHI:

- collects individually identifying health information only as authorized;
- uses individually identifying health information only as authorized;
- obtains individually identifying diagnostic, treatment and care information and registration information from other custodians without consent only as authorized;
- discloses individually identifying diagnostic, treatment and care information, registration information and health services provider information only as authorized;
- maintains privacy and confidentiality and follows policies and procedures as negotiated with the Minister;
- is subject to the oversight of the Information and Privacy Commissioner;
- grants individuals access to their health information (individuals would place the request with the department of Alberta Health and Wellness); and
- cooperates and complies with all orders issued by the Information and Privacy Commissioner.

Health Services Databases Maintained by CIHI

- **Discharge Abstract Database (DAD) and Hospital Morbidity Database**
  This patient-specific database contains clinical, demographic and administrative data on patient discharge including the most responsible physician and diagnosis, the principle procedure performed, the patient gender, date of birth, postal code, hospital number, personal health number and admission discharge data (e.g. admission category, length of stay). All provinces provide data for inclusion in the Hospital Morbidity Database, while reporting data for inclusion in the DAD is optional. Since Alberta facilities provide data for DAD, CIHI also uses this data to populate the Hospital Morbidity Database. This identifiable data is collected at the facility level and sent to CIHI on a monthly basis. Data is generally submitted electronically by tape or modem.

- **Canadian Organ Replacement Register (CORR)**
  This database contains patient-specific data on all dialysis patients who began treatment for renal failure in Canada since 1981, and on organ donation (heart, lung, liver, kidney and pancreas) and extra-renal activities since 1990. Patient demographics (including name,

date of birth, and PHN), treatments received (dialysis and/or transplant), risk factors, and follow-up on graft failures and deaths are also included. Data comes from individuals through the completion of patient-specific forms and also through a facility profile survey. In Alberta, this data is collected at the University of Alberta Hospital and Calgary Regional Health Authority (from the HOPE Program) and forwarded directly from the RHA level to CIHI.

- **Hospital Mental Health Database**
  The Hospital Mental Health Database is based on inpatient events only and excludes patients treated in residential care facilities. Data consists of demographics (age, sex, birth date) and medical diagnosis information. This data is downloaded from DAD if the facilities already report to DAD.

- **National Trauma Registry (NTR)**
  The NTR contains demographic, diagnostic and procedural information on all acute care hospital admissions due to injury. The Minimal Data Set are extracted from the Discharge Abstract Database based on the External Causes of Injury (E Codes) within the International Classification of Diseases (ICD) coding system.

- **Therapeutic Abortions Database**
  The Therapeutic Abortions Database contains patient identifiable demographic information including age and province of residence, medical data including days of care, initial surgical procedure, and sterilization procedure. This data is manually collected at the facility and forwarded to Alberta Health and Wellness. Alberta Health and Wellness converts the data to electronic form. On an annual basis, the data is sent to CIHI on tape. (Individuals obtaining this service as an in-patient would also be reported through the DAD.)

Health Professionals Databases Maintained by CIHI

- **National Physician Database (NPDB)**
  The NPDB contains data on socio-demographic and billing activities of fee-for-service physicians as well as on the age and gender of patients. Alberta Health and Wellness sends electronic file monthly to CIHI. The data is anonymized, based on a unique number that is generated (via constant algorithm) at the national level. This physician number is created in such a way as to follow the physician across provinces for a lifetime. CIHI does not have access to the algorithm and the unique number is scrambled before the file is sent to CIHI. Other potential identifiers such as addresses, postal codes and ages are grouped. CIHI generates reports based on this database, which are then forwarded to Alberta Health and Wellness. Alberta Health and Wellness does not have direct access to the database. Research based requests for access to the database are managed by CIHI with Alberta Health and Wellness having final approval prior to the data actually being released for research purposes.

alberta we//net

alberta we//net is both a branch of the department of Alberta Health and Wellness and an information manager. It is the umbrella under which a series of province-wide and regional initiatives are being developed and carried out to build a secure network that will enable health professionals to share health information.

For each of the projects or initiatives under its umbrella, there should be an agreement under **section 66**. In some cases, the agreement would be with the Minister and in other cases, there may be separate agreements with individual custodians, such as regional health authorities. As an information manager, alberta we//net has to comply with the requirements of the *Health Information Act* and the terms and conditions of its agreement(s) regarding the collection, use, disclosure and protection of health information disclosed to it.

alberta we//net tries to find the best ways to use technology to securely link health professionals and to enable them to share appropriate information with each other. In this way, health services providers and custodians are provided with the best available evidence to make better decisions on how to improve the health of individual Albertans and to manage Alberta's health system as a whole.

The master plan identifies 29 possible province-wide projects to support the sharing of specific information and 14 infrastructure and transition projects to enable information sharing. The following projects are either currently implemented, in progress, or being considered within four broad strategic purposes:

Promoting Health and Well-being

- **Spatial Population Health Information Exchange (SPHINX)** This is a co-operative project between Alberta Health and Wellness and Health Canada. SPHINX securely displays and analyzes information contained in existing databases from many sources in formats such as maps, charts, and graphs. It makes non-identifying health-related data easily, but securely, accessible to public health officials to monitor and report on public health, and analyze the factors influencing health. This information can be used to protect citizens from disease outbreaks, environmental contamination and other potential health dangers. Databases currently available or being considered are Census data, Water Quality, Agriculture Census, Notifiable Diseases, and Vital Statistics – births and deaths.

- **Breast Cancer Screening** At this stage, the project is developing functions to handle the identification and recruitment of women for mammograms in support of the province-wide, population-based Breast Cancer Screening Program that the department is working on with key stakeholders. This program will build on the services currently provided by radiologists, health authorities, and the Alberta Cancer Board. The Breast Cancer Screening Program will establish a consistent, province-wide approach to conducting mammograms for the purpose of breast cancer screening. alberta we//net is providing technical support to this program.

- **Newborn Metabolic Screening and Newborn Registration** These are applications that enable more efficient tracking of metabolic screening by registering newborns at birth with their own unique lifetime identifier number and by the electronic reconciliation of the registration list with the screening samples at the Newborn Metabolic Screening Laboratory. Three types of metabolic conditions that impair mental capacity can be detected through a simple blood test administered no later than seven days after birth. The department has been screening newborns for metabolic conditions since the 1960s. The Newborn Metabolic Screening project supports more effective tracking of newborns to ensure that parents are given the opportunity to have their baby tested following discharge from hospital.

- **Pathology Lab Results for Screening Programs and Cervical Cancer Screening** These are projects that are in the early stages of consideration. alberta we//net will provide technical support through these projects to the department of Alberta Health and Wellness screening programs.

Improving Access

- **Telehealth** This project closes the geographical distance between patients in remote and rural areas and specialists in major centres by making it possible for local doctors and health service providers to consult with their colleagues about diagnostic and treatment via satellite and other telecommunications technologies. Applications of telehealth being deployed or being considered include Psychiatry, Radiology, Consulting (covers a wide range of health specialties, including dermatology, geriatrics, physiotherapy, rehabilitation, and occupational therapy), Ultrasound, Cardiology, and Home Care. Telehealth video-conferencing also provides distance learning and continuing education opportunities to health professionals in rural and remote areas. Telehealth is deployed through various facilities in the 19 health authorities.

Optimizing Quality and Utilization of Health Services

- **Integrated Cancer Care Network** This is a project under the direct management of the Alberta Cancer Board. It supports the development and implementation of cancer treatment protocols – consistent, effective approaches to treat certain types of tumours. These protocols are integrated with an electronic medical record for each patient to facilitate best treatment practices in all treatment centres. The application has been implemented for some specific tumor groups and is being enhanced to support implementation by function, such as patient scheduling.

- **Seniors Drug Profile** This project provides health services providers with information about medication prescribed to Alberta seniors paid for by the department through the Alberta Blue Cross Coverage for Seniors (Group 66) program. This up-to-date patient information, released only with explicit patient consent, enhances the ability of health services providers to carry out effective diagnosis and treatment. The application is deployed or planned to be deployed in various hospital emergency departments, hospital pharmacies and admitting units, and with home care providers and community doctors.

- **Pharmaceutical Information Network** This will link doctors, pharmacies, and health facilities to enable the electronic exchange of medication information, allowing health care providers to have a common picture of each patient's medication profile. It will also provide physicians and pharmacists with current best practices information for medication therapy. The application will equip health care providers with a listing of medications that a patient is taking and why; the medications a patient should be taking; the patient's past medication treatment, allergies and adverse drug events; information on the best medications to treat a particular problem, how much to prescribe, and costs. This application, when deployed, will also implement the infrastructure for secure information exchange for future applications.

- **Lab Test Results** This information will be made available to health services providers along with the Pharmaceutical Information Network. This is similar to the access to medication histories provided by Seniors Drug Profile, and responds to requests from health service providers for quicker access to a patient's latest lab test results.

Improving Health System Management and Accountability

- **Common Opportunities** These are initiatives where health system stakeholders work together to enhance their internal computer systems and infrastructure. alberta we//net facilitates and supports the process. The objective is to strengthen the management tools available to stakeholders and enable secure information exchange to take place in a cost-effective manner.
- **Common Opportunities for Health Authorities** All regional health authorities have either completed or are participating in common opportunity projects to strengthen their administrative and clinical systems. Three new health authority common opportunities are being considered: human resource systems, shared services, and the use of a provincial person health identifier across the health system.
- **Common Opportunities for Physician Office Systems** alberta we//net is working with doctors to help them assess the benefits and costs of automation and alternate methods of delivering physician office systems to physician clinics. Physician office automation will enable doctors to take full advantage of alberta we//net applications. The physician office system software enables the automation of the business and clinical aspects of a physician's practice through such computer functions as electronic medical records, billing and appointment scheduling, and access to information for professional development. aberta we//net has conducted two pilots of physician office automation, first to evaluate the changes required in business and patient care processes in order to implement electronic medical records and billing and scheduling software, and second to implement and evaluate remote access by physicians to a physician office system as an alternative to implementing the system physically within a clinic.

- **Network Infrastructure** The Government of Alberta's wide-area network, AGNpac, provides the 'information highway' to support alberta we//net initiatives. Access to the network is provided by connection access points that act like 'entrance ramps' and are distributed geographically across the province. This is how health authorities and other public sector stakeholders have access to alberta we//net. The development of Alberta's new high-speed network ('supernet') over the next three years, will help address barriers and open new opportunities for information exchange in the health sector.

5.3.3 POWER TO CHARGE FEES

Under **section 67(1),** custodians have the power to charge the fees set out in the Health Information Regulation for services provided under **Part 2 of the *Act* (Individual's Right to Access Individual's Health Information)**. The fees apply to the processing of requests by an applicant for access to a record containing health information. In accordance with **section 67(2)** of the *Act* and section 9 of the Regulation, they include both a basic fee of $25.00 for performing the steps involved in producing a copy of the information, and additional fees in accordance with the **Fee Schedule** in the Regulation**.** The basic fee is called an initial fee under the *FOIP Act* but only applies to access to general records, not to personal information, under that *Act*.

Section 67(3) says that a custodian must give an applicant an estimate of the total fee for its services before providing the services. **Section 10** of the Regulation sets out what needs to be included in a fee estimate and gives an applicant up to 20 days to indicate if the fee estimate is accepted or to modify the request to change the amount of fees assessed.

Section 11(1) of the Regulation states that processing of a request ceases once a notice of estimate has been forwarded to an applicant and starts again immediately upon the receipt of an agreement to pay the fee and on the receipt of at least 50% of any estimated fee. The balance of any fee owing is payable at the time the information is delivered to the applicant **(section 11(2)** of the Regulation).

Section 67(6) says that the fees must not exceed the actual cost of the service. If the amount paid is higher than the actual cost of the service, all or part of the fees will be refunded by the custodian **(section 11(3)** of the Regulation).

Section 67(4) allows a custodian to excuse an applicant from paying all or part of a fee if, in the custodian's opinion, the applicant cannot afford the fee or in any other circumstances provided for in the regulations. For the purposes of this section of the *Act*, **section 12** of the Regulation permits a custodian to excuse an applicant from paying all or part of a fee if, in the opinion of the custodian, it is fair to excuse payment.

If the custodian refuses an applicant's request to excuse the payment of all or part of a fee, the custodian must notify the applicant that the applicant may ask for a review by the Commissioner **(section 67(5))**.

For a more detailed discussion on Estimating, Assessing and Excusing Fees, see section 2.5.8 of Chapter 2 of this Publication.

5.4 DATA MATCHING RULES

Division 2 of Part 6 of the *Act* (Duties and Powers of Custodians Relating to Data Matching – Data Matching) enables custodians to perform data matching. However, because of the possibility of taking otherwise non-identifying health information and combining it creates information that potentially identifies individuals, that **Division** sets out specific rules and controls over data matching.

"Data matching" is defined in **section 1(1)(g)** of the *Act* to mean the creation of individually identifying health information by combining individually identifying or non-identifying health information or other information from 2 or more electronic databases, without the consent of the individuals who are the subjects of the information.

Related to data matching is **"data linkage"** or **"data profiling"** which is a computerized use of health information and other personal data from a variety of sources, to merge and compare files on identifiable individuals or categories of individuals. This linkage or profiling creates a new body of health information.

5.4.1 GENERAL PROHIBITION RESPECTING DATA MATCHING

Under **section 68,** a custodian must not collect the health information to be used in data matching, or use or disclose the health information to be used in data matching or created through data matching in contravention of the *Act*.

It is an offence under **section 107(2)(a)** for any person to knowingly collect, use, disclose or create health information in contravention of this *Act*.

There must be authority for the collection, use or disclosure of individually identifying health information being used for data matching or that is being created as a result of the data matching.

Some of the matters that should be considered before and during any data matching project are:

- Is there a data matching policy and guidelines in place within the custodian? Have they been followed?
- Has the data matching been authorized by an appropriate designated official within the custodian?
- Will the information generated or created by the matching program be verified against original or additional authoritative sources before the information is used for an administrative purpose, especially if it impacts an individual?
- Has there been an assessment of the advantages of the proposed matching against alternative control, management or enforcement approaches?
- Has there been an assessment of how the information is to be collected and how the information created through the data matching is to be used and disclosed?

5.4.2 DATA MATCHING WITHIN A CUSTODIAN

A custodian may perform data matching using information that is in its custody or under its control **(section 69)**. There is no requirement in the *Act* to prepare a privacy impact assessment for this type of data matching, provided the data matching is being done for an authorized purpose **(section 27)** and will not result in a use of individually identifying health information that will affect the privacy of the individual who is the subject of the information.

5.4.3 DATA MATCHING BETWEEN CUSTODIANS

However, if a custodian wishes to perform data matching by combining information that is in its custody or under its control with information that is in the custody or under the control of another custodian it must meet the requirements of **section 70(2) and (3)**. The requirements are:

- before performing data matching, the custodian in whose custody and control the information that is created through data matching will be stored must prepare a privacy impact assessment and submit the assessment to the Commissioner for review and comment; and
- the privacy impact assessment must describe how the information to be used in the data matching is to be collected, and set out how the information that is created through data matching is to be used or disclosed.

Section 70(3) sets the minimum requirements for PIAs for data matching projects. Custodians should follow the PIA process set out in **section 5.2.8 of this Chapter**.

5.4.4 DATA MATCHING BETWEEN A CUSTODIAN AND A NON-CUSTODIAN

If a custodian wishes to perform data matching by combining information that is in its custody or under its control with information that is in the custody or under the control of a non-custodian, the custodian must meet the requirements in **section 71(2) and (3)**. The requirements are:

- before performing data matching, the custodian must prepare a privacy impact assessment and submit the assessment to the Commissioner for review and comment; and
- the privacy impact assessment must describe how the information to be used in the data matching is to be collected, and set out how the information that is created through data matching is to be used or disclosed.

If a non-custodian wants to collect individually identifying health information for a data matching purpose, the disclosing custodian must follow the rules under the *Health Information Act* for such a disclosure.

It is an offence under **section 107(5)** for a non-custodian who receives non-identifying health information and who intends to use the information to perform data matching, to fail to comply with **section 32(2)**. Under that **section,** the disclosing custodian must inform the person that the person must notify the Commissioner of an intention to use the information for data matching, before performing the data matching.

5.4.5 DATA MATCHING FOR RESEARCH PURPOSES

Under **section 72,** if data matching is performed for the purpose of conducting research, **sections 48 to 56** must be complied with before the data matching is performed. A privacy impact assessment is also required. **Sections 48 to 56** require the review, by an ethics committee, of a research proposal for the disclosure of health information, including an assessment of public interest, privacy impacts and security safeguards; an application to the custodian for disclosure of health information for research purposes; and the terms and conditions of an agreement that must be entered into with the researcher.

Refer to section 5.2.8 of this Chapter for a detailed discussion of the Duty to Prepare Privacy Impact Assessments and to section 8.15 of Chapter 8 for a discussion on Disclosure for Research Purposes.

THINGS TO REMEMBER

DUTIES AND POWERS OF CUSTODIANS RELATING TO HEALTH INFORMATION

- The duties of custodians encompass a set of fair information practices for health information. They apply throughout the *Act* to all custodians and to their affiliates.

- A custodian must collect, use and disclose health information at the highest level of anonymity possible. A custodian must first consider whether aggregate health information or non-identifying health information would be adequate for the intended purpose. If neither level of anonymity would be adequate for the intended purpose, the custodian may collect, use or disclose individually identifying health information if it is authorized by the *Health Information Act* and is carried out in accordance with the *Act*. The duty to collect, use or disclose health information at the highest level of anonymity does not apply where collection, use or disclosure is for the purpose of providing a health service or determining eligibility.

- Anonymous health information means either aggregate or individual anonymous information.

- Aggregate health information means non-identifying health information about groups of individuals with common characteristics.

- Non-identifying health information means that the identity of the individual who is the subject of the information cannot be readily ascertained from the information.

- Individually identifying health information means that the identity of the individual who is the subject of the information can be readily ascertained from the information.

- The identity of an individual can be said to be readily ascertained if:

an individual's identity can be determined by combining available data or information within the same or in several different records held by the same custodian;

an individual's identity can be determined by comparing information representing distinguishing characteristics with other information sources having both the distinguishing characteristics and the names or other identifiers of individuals; and

only readily available or conventional computer hardware, software and technical expertise is used.

- A custodian may use processes to transform individually identifying health information to make it non-identifying (e.g. stripping identifiers, encrypting, aggregating information, etc.).

- A custodian may enter into an agreement with an information manager (a special type of affiliate) to process, store, retrieve, dispose of or transform health information or to provide information management or information technology services. (See Components for an Agreement with an Information Manager in Appendix 4 of the Manual).

- A custodian that has entered into an agreement with an information manager may disclose health information to the information manager without the consent of individual subjects for the purposes authorized by the agreement.

- A custodian must collect, use or disclose only the amount of health information essential to enable the custodian or recipient to carry out the intended purpose.

- In deciding how much health information to disclose, a custodian must consider any expressed wishes of the individual relating to disclosure of the information together with any other relevant factors.

- A custodian must obtain an individual's consent to the disclosure of his/her individually identifying diagnostic, treatment and care information by "electronic means" or ensure that the individual's consent has been previously obtained, prior to disclosing the information (unless the

disclosure is for the purpose of obtaining or processing payment for a health service). "Electronic means" is defined in the Health Information Regulation as a computer system that facilitates access by authorized persons to a custodian to electronic or digital information that is stored in a computer database by a custodian. (See section 5.2.3 of Chapter 5 for a discussion of consent to disclosure by electronic means).

- A custodian must take reasonable steps to maintain administrative, technical and physical safeguards to ensure compliance with the *Act* by the custodian and its affiliates and to protect:

    the confidentiality of health information in its custody or under its control and the privacy of the individual subjects;

    the confidentiality of health information that is to be stored or used outside Alberta or that is to be disclosed by the custodian to a person outside Alberta and the privacy of the individual subjects (unless the health information is used solely for the purpose of providing continuing treatment or care to the individual);

        against any reasonably anticipated threat or hazard to the security or integrity of the information or of loss of health information or unauthorized access to, use, disclosure or modification of the health information.

- A custodian must maintain safeguards for proper disposal of records to prevent any reasonably anticipated unauthorized access to, use or disclosure of the health information.

- In order to assess the level and type of safeguards needed to protect health information, a custodian should conduct a threat and risk assessment of the health information in its custody or under its control. (See Chapter 11 of the Manual re Conducting a Threat and Risk Assessment).

- A custodian should establish a health information security policy and ensure that its affiliates are aware of and comply with the policy. (See Chapter 11 of the Manual for the Components of a Health Information Security Policy).

- Before using or disclosing health information in its custody or control, a custodian must make reasonable efforts to ensure that the information is accurate and complete.

- A custodian must identify its affiliates who are responsible for ensuring that the *Act,* the regulations and the policies and procedures of the custodian related to health information are complied with.

- A custodian must establish or adopt policies and procedures that will facilitate the implementation of the *Act* and regulations.

- Any collection, use or disclosure of health information by an affiliate of a custodian is a collection, use or disclosure by the custodian.

- Any disclosure of health information to an affiliate of a custodian is a disclosure to the custodian.

- A custodian must prepare a privacy impact assessment whenever a proposed change to an administrative practice or proposed new or modified information system relating to the collection, use or disclosure of individually identifying health information may affect the privacy of individual subjects. The privacy impact assessment must be submitted to the Commissioner for review and comment before the custodian implements the proposed practice or system. (See section 5.2.8 of Chapter 5 regarding the Duty to Prepare Privacy Impact Assessments and Chapter 11 of the Manual for a *Health Information Act* Privacy Compliance Checklist).

- Before matching health information in its custody or control with information in the custody or under the control of another custodian or non-custodian, the custodian must prepare a privacy impact assessment and submit it to the Commissioner for review and comment. If the data matching is performed for research purposes, sections 48 to 56 of the *Act* must also be complied with.

THINGS TO REMEMBER

CONSENT UNDER SECTION 59

When is Consent under Section 59 Required?

Section 59(1) requires a custodian to obtain consent from an individual before disclosing individually identifying diagnostic, treatment and care information by "electronic means" or to ensure that consent for this form of disclosure has already been obtained. "Electronic means" is defined in the *Health Information Act* Regulation as "a computer system that facilitates access by authorized persons to electronic or digital information that is stored in a computer database by a custodian". (See the Section 59 Consent Form in Appendix 1 of the Manual). In plain language, this means that a custodian must obtain consent before disclosing individually identifying diagnostic, treatment and care information that will be obtained (by another custodian) by accessing a database through a computer network.

An example would be disclosure of an individual's diagnostic, treatment and care information, including drug information, to alberta we//net's proposed Pharmaceutical Information Network. Doctors, pharmacies, pharmacists and health facilities will be able to access that database and exchange the individual's health information with other custodians electronically.

What Must Be Included in Consent Under Section 59?

- Authority for any custodian to disclose individually identifying diagnostic, treatment and care information about the individual by electronic means for all the *section 27* authorized purposes;
- Acknowledgment that the individual has been made aware of the reasons for disclosure by electronic means and the risks and benefits to the individual of consenting or refusing to consent;
- The date the consent is effective; and
- A statement that the consent may be revoked at any time by the individual.

The consent or revocation of consent must be in writing or provided electronically. If the consent is written, it must be signed by the person providing it.

When is Consent under Section 59 Not Required?

Consent under this section is not required when the disclosure by electronic means is for the purpose of obtaining or processing payment for health services (e.g. if a pharmacist discloses information to a third party insurer or drug plan carrier for billing or claims payment purposes) (section 59(7)).

See the discussion on Consent for Disclosure by Electronic Means in section 5.2.3 in Chapter 5.

CHAPTER SIX

COLLECTION OF HEALTH INFORMATION

6.1 OVERVIEW OF CHAPTER SIX

This Chapter will cover:

- the limits on the collection of health information;
- the duties of custodians collecting health information;
- the collection of non-identifying health information;
- the authority to collect individually identifying health information;
- the persons who can require individuals to provide their personal health number;
- the duty to collect individually identifying health information directly from the individual it is about;
- the authority for indirect collection of health information;
- the requirement to obtain consent before using a recording device; and
- the application of the 'need to know' principle to the collection of health information by affiliates.

6.2 LIMITS ON COLLECTION

The rules governing the collection of health information are found in **Part 3 (Collection of Health Information)** of the *Act* **(sections 18 to 24)** and also within the duties of custodians relating to health information in **Part 6** of the *Act* **(sections 57 and 58)**. **"Collect"** means to gather, acquire, receive or obtain health information **(section 1(1)(d))**. Collection can include activities such as taking a medical history; having individuals respond through surveys, questionnaires or polling, or having individuals complete forms to provide health information. The collection may be done in writing, by audio or video taping, by electronic data entry, over the telephone or by other means.

Custodians are bound by the requirements of the *Act* whether the collection activities are carried out by the custodian or by its affiliates.

There are a number of specified limitations on collection in the *Act*, particularly those related to the collection of individually identifying health information and also to the collection of personal health numbers.

A general prohibition on the collection of health information is set out in **section 18**. That section says that custodians must not collect health information except in accordance with the *Act*.

6.2.1 DUTY TO COLLECT HEALTH INFORMATION WITH THE HIGHEST DEGREE OF ANONYMITY

Custodians collecting health information must consider the intended purpose for the collection and the level of anonymity that is needed for that intended purpose. They must first consider whether collection of aggregate health information will be adequate for the intended purpose and if so, must collect only aggregate health information **(section 57(2))**.

"Aggregate health information" is defined in **section 57(1)** to mean non-identifying health information about groups of individuals.

If the custodian believes that collecting aggregate health information will not be adequate for the custodian's intended purpose, the custodian must then consider whether collection of other non-identifying health information is adequate for the intended purpose, and if so, the custodian may collect other non-identifying health information **(section 57(3))**.

"Non-identifying health information" is defined in **section 1(1)(r)** to mean that the identity of the individual who is the subject of the information cannot be readily ascertained from the information.

Under **section 57(4),** if the custodian believes that collecting aggregate and other non-identifying health information will not be adequate for the custodian's intended purpose, the custodian may collect individually identifying health information if the collection is:

- authorized by the *Health Information Act*; and
- carried out in accordance with the *Health Information Act.*

Under **section 65,** a custodian may strip, encode or otherwise transform individually identifying health information to create non-identifying health information.

"Individually identifying health information" is defined in **section 1(1)(q)** to mean that the identity of the individual who is the subject of the information can be readily ascertained from the information.

"Readily ascertained" in the context of **section 57,** means that the identity of an individual (e.g. the individual's name or other identifiers or distinguishing characteristics associated with an individual) can be determined or deduced without having to apply a sophisticated technical method or process, or without having the particular technical expertise to do so.

An individual's identity can be said to be "readily ascertained" if his or her identity can be determined by:

- combining available information within the same or in several different records;
- comparing information representing distinguishing characteristics with other information sources having both the distinguishing characteristics and the names or other identifiers of individuals; and
- if only readily available or conventional computer hardware, software and technical expertise is used.

Section 57 does not apply where the collection of health information is for the purpose of providing a health service (as defined in **section 1(1)(m)**), or for determining the eligibility of an individual to receive a health service.

See section 5.2.1 of Chapter 5 of this Publication for a more detailed discussion of this duty.

6.2.2 DUTY TO COLLECT HEALTH INFORMATION IN A LIMITED MANNER

In addition to complying with **section 57,** custodians must collect only the amount of health information that is essential to enable the custodian or the recipient of the information to carry out the intended purpose **(section 58(1))**.

See section 5.2.2 of Chapter 5 of this Publication for a more detailed discussion of this duty.

6.2.3 APPLYING THE 'NEED TO KNOW' PRINCIPLE TO THE COLECTION OF HEALTH INFORMATION BY AN AFFILIATE

The *Health Information Act* limits the authority of affiliates to collect health information. Under **section 24,** an affiliate of a custodian must not collect health information in any manner that is not in accordance with the affiliate's duties to the custodian.

This means that unless the information is necessary for the affiliate to carry out his/her/its designated responsibilities, the affiliate should not be collecting that information. This also implies that custodians must identify the roles and responsibilities of their affiliates and ensure that affiliates are informed about these duties and responsibilities.

Affiliates must also understand that their roles and responsibilities will limit the amount and type of health information they will need to collect.

For example, a receptionist at the front counter of a clinic may only need to collect the name, address, phone number and personal health number of a patient attending the clinic for the first time. This would be needed to set out the patient's chart and for billing purposes.

Depending upon the role of a physician's nurse, the nurse might collect a history and other basic health information such as the patient's complaint or presenting symptoms, and height, weight, blood pressure, etc.

The physician would collect a complete medical (and perhaps family and genetic) history.

6.3 COLLECTING NON-IDENTIFYING HEALTH INFORMATION

Custodians may collect non-identifying health information for any purpose **(section 19)**.

Practically speaking, health information is really only non-identifying information if the custodian or other person or entity receiving the information does not have other information that could, in combination, identify an individual.

6.4 AUTHORITY TO COLLECT INDIVIDUALLY IDENTIFYING HEALTH INFORMATION

Under **section 20,** custodians may only collect individually identifying health information if:

- the collection of that information is expressly authorized by an enactment of Alberta or Canada; or
- the information relates directly to and is necessary to enable the custodian to carry out a purpose authorized under **section 27**.

Collection Expressly Authorized by an Enactment of Alberta or Canada (section 20(a))

This means that a statute of Alberta or Canada or a regulation made under a federal or Alberta statute provides for the collection of individually identifying health information. In some cases, a statute both authorizes collection and identifies the health information that may be collected. More commonly, the statute will authorize a program or activity to be carried out and a regulation under the statute will authorize the collection of individually identifying health information needed for the program or activity and sometimes the form or format in which the information is to be collected.

An example of a statute authorizing collection of individually identifying health information would be **section 31** of the *Public Health Act* which requires individuals to consult with a physician or attend a sexually transmitted disease clinic if they know or have reason to believe they may have a communicable or sexually transmitted disease. This section would authorize a custodian to collect individually identifying health information to determine whether the individual has such a disease. The regulations under the *Act* specify the diseases to which the requirement applies.

An example of a regulation authorizing collection would be **section 21(1)** of the Health Insurance Premiums Regulation that requires residents of Alberta to register themselves and their dependents with the Minister on the prescribed form.

If an enactment authorizes a program or activity but there is no specific or express authority for the collection of information for the purposes of the program or activity, a custodian cannot rely on the enactment as authority for collection of the information.

The principles of collecting the least amount of information at the highest level of anonymity continue to apply. Even if collection is authorized by another enactment, the custodian must collect the least amount of information necessary and if identifying information is not needed for the specific purpose, it must not be collected.

Collection Necessary to Carry Out a Purpose Authorized under Section 27 (section 20(b))

If the individually identifying health information is directly related to **and** necessary for a custodian to carry out a specific function outlined under **section 27**, the custodian is authorized to collect it.

"Relates directly to" means that the individually identifying health information has a direct bearing on the program or activity.

"Necessary for" means being able to demonstrate that individually identifying health information is needed to carry out one of the functions or purposes under **section 27**.

The collection must meet both parts of the two-part test above in order for a custodian to rely on **section 20(b)** as authority for the collection.

Some of the purposes for which a custodian may collect individually identifying health information as set out in **section 27(1)** include:

- providing health services ("health service" is defined in **section 1(1)(m)**);

- determining eligibility to obtain health services (e.g. for the Alberta Aids to Daily Living Program);
- investigating, reviewing or inspecting the services provided by health service providers (e.g. for professional regulatory bodies and other review bodies to investigate complaints);
- conducting research **(note definition of "research" in section 1(1)(v))**;
- providing health service provider education (e.g. for the creation of case studies for review in medical grand rounds);
- carrying out specific purposes identified in other legislation (e.g. *Hospitals Act, Cancer Programs Act, Regional Health Authorities Act, Public Health Act*); and
- internal management including planning, resource allocation, policy development, quality improvement, monitoring, audit, evaluation, reporting, obtaining or processing payment for health services and human resource management.

Some custodians (the Minister and Department, regional health authorities, the Alberta Cancer Board and the Alberta Mental Health Board) may also collect individually identifying health information that is directly related to and necessary for the following purposes:

- planning and allocating resources on a regional or provincial basis (e.g. provincial costing project, development of alternate payment plans for physicians, conducting surveys about health system performance);
- managing the health system on a regional or provincial basis (e.g. supporting medical and hospital reciprocal agreements, managing physical therapy and home care programs);
- conducting public health surveillance to determine and improve the health of the regional or provincial population (e.g. assessing environmental health hazards, identifying contacts of individuals with communicable diseases); and
- developing health policies and programs on a regional or provincial basis (e.g. analyzing utilization of programs and treatments to identify trends, developing programs for specific target groups such as aboriginal groups, children, seniors, etc.) **(section 27(2))**.

See Chapter 7 of this Publication (Use of Health Information) for a more detailed discussion of section 27 purposes.

BEST PRACTICE: *Custodians should regularly review their collection of individually identifying health information to ensure that the collection falls within* ***section 20(a)*** *or* ***(b)*** *and to eliminate any unnecessary collections. If a custodian stops collecting certain individually identifying health information, the collection instruments (forms, surveys, etc.), contracts and procedures requiring this collection should be amended. Custodians should also ensure that information needed for subsets of clients is collected only for those clients.*

Administrative controls should be implemented to ensure that all new or modified collections of individually identifying health information meet the criteria set out in ***section 20*** *and that the minimum information needed to meet program needs is collected.*

If irrelevant individually identifying health information is collected, it should be placed in a separate file or electronic location to ensure that it is not improperly used and that it is destroyed at an appropriate time

after completion of the process for which the information was inadvertently collected.

New collection activities and instruments should be reviewed by the Health Information Coordinator or whoever carries out those duties and responsibilities.

6.5 COLLECTING PERSONAL HEALTH NUMBERS

The inappropriate use of personal health numbers can have a negative impact on an individual's privacy. The personal health number provides a single point of access to that individual's identifying health information and is therefore, a single point of risk. The *Health Information Act* intentionally limits the collection of personal health numbers by specifying in **section 21(1)** who can require an individual to provide their personal health number. The *Act* also gives individuals the right to refuse to provide their personal health number to any person who is not referred to in that section **(section 21(3))**. Those other persons may ask an individual for his or her personal health number but they do not have the right to require the individual to provide it.

Other statutes, such as the *Canada Health Act,* ensure that individuals cannot be refused necessary health services even if they cannot provide their personal health numbers. This situation could arise where for example, an injured student is brought by a teacher to a medical clinic for treatment and the parent has not previously provided the school with the child's personal health number.

6.5.1 RIGHT TO REQUIRE PROVISION OF PERSONAL HEALTH NUMBER

Only custodians and persons authorized by the regulations have the right to require an individual to provide the individual's personal health number **(section 21(1))**. Under **section 5** of the **Regulation,** the following persons are authorized to require individuals to provide their personal health numbers:

- the Students' Finance Board for the purpose of administering student health benefits programs;
- lawyers and insurers for the purpose of enforcing the Crown's right of recovery under Part 5 of the *Hospitals Act;*
- insurers for the purpose of facilitating the handling, assessing and payment of claims for benefits;
- The Workers' Compensation Board for the purpose of facilitating the handling, assessing and payment of claims for benefits;
- ambulance attendants and operators under the *Ambulance Services Act* for the purpose of providing health services to individuals and seeking reimbursement for providing those services from the Alberta Blue Cross Plan;
- the Minister of Justice and Attorney General for the purpose of providing health services to an inmate outside of a correctional institution;
- the Minister of Community Development for the purpose of administering the *Seniors Benefit Act;*
- the Minister of Human Resources and Employment for the purpose of administering the income and employment programs of the

Department of Human Resources and Employment; and
- persons, other than custodians, who provide health services to individuals for the purpose of seeking reimbursement for providing those services from the Alberta Health Care Insurance Plan.

"Insurer" is defined in **section 5(1)** of the **Regulation** as the ABC Benefits Corporation or an insurer licensed under the *Insurance Act.*

Notice to Individual

Custodians and the persons listed in **section 5** of the **Regulation** must advise individuals of their authority to collect personal health numbers under **section 21** before they request a personal health number from an individual **(section 21(2))**.

Right to Refuse to Provide Personal Health Number

Individuals can refuse to provide their personal health number if someone other than custodians or those listed in the regulation asks for it **(section 21(3))**. However, they can continue to provide their child's number, if they wish, to babysitters or day care centers. School jurisdictions, municipalities and post-secondary institutions, subject to the *FOIP Act,* do not have the authority under that legislation to collect the personal health number and are not listed in **section 5** of the **Regulation** as persons who may require the provision of the personal health number.

6.6 MANNER OF COLLECTION

The *Act* sets out the manner in which the collection of health information must take place. This includes the duty of custodians to collect health information from the subject individual; the exceptions to this duty; and the notice that must be given to the individual about the collection.

6.6.1 DUTY TO COLLECT DIRECTLY FROM INDIVIDUAL

Section 22(1) states that, subject to some limited exceptions, a custodian must collect individually identifying health information directly from the individual who is the subject of the information.

Direct collection is the primary method for obtaining individually identifying health information. This helps to ensure that an individual is aware of the type of health information being used, how it will be used and by whom. Even where a custodian may have the capability to collect individually identifying health information from another source, it should not do so unless indirect collection is authorized under **section 22(2)**.

6.6.2 AUTHORITY FOR INDIRECT COLLECTION

Section 22(2) of the *Act* provides for a number of circumstances where individually identifying health information may be collected from a person other than the individual who is the subject of the information collection.

***BEST PRACTICE:** When collecting information from someone other than the individual it is about, especially a family member or relative, they should be informed that the individual has a right to access any of their own health information subject to the exceptions in **section 11**. Under that section, a custodian may refuse to disclose health information to an applicant if the disclosure could reasonably lead to the identification of a person who provided health information to the custodian explicitly or implicitly in confidence and in circumstances in which it was appropriate that the name of the person who provided the information be kept confidential.*

If disclosure of the information collected or identifying the source of the information to the individual that it is about could place the informant or someone else at risk of serious harm, the informant should advise the custodian and the custodian should take additional steps to protect the identity of the informant.

Some steps that could be taken would be: avoiding identifying other sources in patient records (if this is feasible);organizing documentation so that information from other sources is separate from the patient's information and easily identifiable; and if disclosure of an informant's identity could cause harm to that individual, document this on the patient's file as well as why the information needs to be kept confidential.

Some circumstances where indirect collection is authorized are:

- **Where the Individual Authorizes Collection from Someone Else (Section 22(2)(a))**

  Information may be provided by someone else orally, through written correspondence, electronic information exchange or file transfer.

***BEST PRACTICE:** When an individual authorizes collection from another source, the authorization should be in writing. This could be a signed authorization form or a letter giving authorization. If the authorization is provided over the telephone, custodians should document the conversation and, whenever possible, send a letter to the individual concerned setting out what he or she has authorized.*

When an individual is asked to authorize an indirect collection, the person should be informed of the nature of the information to be collected, the purpose of the indirect collection and the reasons for making the collection indirectly, and the consequences of refusing to authorize the indirect collection.

- **Where the Information is Collected from the Individual's Representative (Section 22(2)(b))**

  If an individual who is the subject of the information is unable to provide the information, the custodian can collect the information from a person referred to in **section 104(1)(c)** to **(i)** who is acting on behalf of that individual.

  Representatives can include a guardian of an individual under 18; a personal representative of a deceased individual over age 18; a guardian or trustee appointed for an individual under the *Dependant Adults Act;* an agent designated under the *Personal Directives Act;* an individual who has been granted a power of attorney; or the nearest relative of a formal patient under the *Mental Health Act*.

If an individual is being represented by a another person under **section 104 (1)(c)** to **(i),** it may be necessary for a custodian to collect demographic information about the representative. The principles of least amount of information and need to know will need to be applied in this situation.

- **Where Direct Collection Would Prejudice the Interests of the Individual, the Purposes of Collection or the Safety of Another Individual (Section 22(2)(c))**

A custodian may collect individually identifying health information indirectly where the custodian believes, on reasonable grounds, that collection from the subject individual would prejudice the interests of the individual; the purposes of collection; or the safety of any other individual; or would result in the collection of inaccurate information.

Examples of this would be:

- where a patient may not be honest with a custodian. Necessary, accurate information about the patient's health, effectiveness of medication may, therefore, not be obtained;
- where a patient is likely to modify his or her behavior in such as way that it could prevent an effective diagnosis or assessment of the patient's treatment;
- where an individual does not know the information that is needed (e.g. a senior dealing with a pharmacist and neither the senior nor the pharmacist is aware of all the medications the senior may be taking;
- direct collection would delay the provision of emergency treatment;
- requesting the information could cause the individual to react violently; or
- in the case of a psychotic patient, another person's perspective on symptoms and the effect of a particular medication may be required.

"On reasonable grounds" means using logical, sensible or rational thought as the basis for drawing a fair conclusion on a matter.

"Inaccurate information" refers to information that is wrong, incomplete or misleading or information that does not reflect the truth.

- **Where Direct Collection is not Reasonably Practicable (Section 22)(2)(d))**

"Not reasonably practicable" refers to something that is not feasible or possible from a practical standpoint.

Examples of situations where direct collection would not be reasonably practicable are:

- an individual is unconscious;
- the custodian may not have any direct contact with the person; or
- an individual is not capable of understanding why certain information needs to be collected or may be unwilling or unable to provide the information (e.g. admission of a patient to a hospital under **Part 1** of the *Mental Health Act*);

- **Where Collection is for the Purpose of Assembling a Family or Genetic History in the Context of Providing a Health Service to the Individual (Section 22(2)(e)(i))**

A custodian may collect individually identifying health information about family members or other relatives of an individual for the purpose of assembling a family or genetic history where the information collected is to be used in the context of providing a health service to the individual who is the subject of the information.

"Genetic history" refers to the gathering of the medical history of an individual's ancestors to determine whether there are any inherited physical or mental characteristics that may lead to the development of a certain illness or medical condition in the individual.

The information can only be collected under the authority of this section in the context of providing a health service to the individual it is about. It cannot be collected for research or other purposes without the individual's authorization.

- **Where Collection is for the Purpose of Determining the Individual's Eligibility to Participate in a Program or to Receive a Benefit (Section 22(2)(e)(ii))**

This section provides authority for indirect collection where a custodian is determining the eligibility of an individual to participate in a program or to receive a benefit, product or health service from a custodian and the information is collected in the course of processing an application made by or for the individual who is the subject of the information.

Certain programs of custodians may have eligibility criteria that must be met in order for an individual to participate in them or receive a benefit or service. This may require the custodian to approach several different sources of information besides the individual to determine whether the criteria or qualifications are met.

Examples include determination of residency status for enrollment in the Alberta Health Care Insurance Plan; assessment of an individual's level of disability for the Alberta Aids to Daily Living program; determination of eligibility for receiving certain drug treatment programs; and assessment of need for Home Care programs.

This collection can only take place in the course of processing an application from the individual, or from his or her representative.

***BEST PRACTICE:** It is a good business practice to inform the individual about whom the information is being collected that information from a variety of sources will be collected to document a particular application. A statement of consent, signed by the individual can be included on the application form but is not absolutely necessary.*

- **Where Collection is for the Purpose of Verifying the Individual's Eligibility to Participate in a Program or to Receive a Benefit (Section 22(2)(e)(iii))**

  This section provides authority for a custodian to verify the eligibility of an individual who is already participating in a program or receiving a benefit, product or health service from a custodian to participate (or continue to participate) in the program or to receive (or continue to receive) the benefit, product or service.

  This provision is intended to allow for cases where an individual has already qualified for a program, benefit, product or service and the custodian needs to check or verify whether the eligibility remains valid. In this case, individually identifying health information may be collected from a variety of sources other than the individual the information is about and the individual may not be informed that verification is taking place.

  For example, random checks of sources of information on the income and assets of individuals on social assistance may be made to determine whether an individual remains eligible for non-payment of Alberta Health Care Insurance premiums.

BEST PRACTICE: *It is a good business practice to inform the individual about whom the information may be collected that verification of continuing eligibility may occur without notice. This is especially necessary if the individual may incur any penalty for receiving a benefit for which he or she has become ineligible.*

- **Where Collection is for the Purpose of Informing the Public Trustee or the Public Guardian about Clients or Potential Clients (Section 22(2)(e)(iv))**

  The Public Trustee is the trustee for dependent adults who are unable to administer their own financial affairs because of a mental disability. The Public Trustee also administers the estates of persons who die without a will if the deceased persons have no adult beneficiaries residing in the province. This office also protects the assets and financial interests of missing persons and children under 18 years of age.

  The Public Guardian is charged with the responsibility of ensuring that appropriate surrogate decision-making mechanisms, supports and safeguards are available to assist adults who are unable to make personal decisions independently.

  This provision permits individually identifying health information to be collected indirectly from relatives, friends and others about anyone who is or may become a ward of the Public Trustee or Public Guardian. This may include information about the individual's mental and physical health.

- **Where the Information is Available to the Public (Section 22(2)(f))**

  This section provides authority for a custodian to collect individually identifying health information indirectly without the consent or knowledge of the individual where the information has been published in any form or is a part of a record that is publicly available.

"Available to the public" refers to information that can be readily found in published or other public sources.

"Published in any form" means in print form or in some other generally accessible form such as an audiotape or videotapes. Examples include birth, marriage or obituary notices, newspaper reports, clipping files and articles in periodicals. Most of this information would be readily available in a public or specialized library.

"Other public sources" refer to recorded information available for a fee or for free, such as information that is available on the Internet, a written biographical sketch provided to participants at a public function, or information in public registry records.

Information of a more private character, based upon personal acquaintance, friendship, observation or gathered through surveillance, would not be included.

- **Where Disclosure is Authorized under Part 5 (Section 22(2)(g))**

A custodian may collect individually identifying health information indirectly (e.g. from another custodian) where the other custodian or other source has authority to disclose it under **Part 5** of the *Act* **(Disclosure of Health Information).**

Without this provision, a custodian might not have any authority to collect or receive the information that is disclosed to it in an authorized way. The provision also assists in eliminating the need for duplicate collection of the same information that has already been disclosed to the custodian.
For example, an individual may have already consented to the disclosure of his or her individually identifying diagnostic, treatment or care information to the custodian who needs to collect this information; the disclosure is to a person authorized to conduct an audit of the information, under certain conditions; or the disclosure is to a quality assurance committee within the meaning of **section 9** of the *Alberta Evidence Act.*

6.6.3 NOTIFYING THE INDIVIDUAL ABOUT THE COLLECTION

Section 22(3) states that when collecting individually identifying health information directly from the individual it is about, the custodian must take reasonable steps to inform the individual about:

- the purpose for which the information is collected;
- the specific legal authority for the collection; and
- the title, business address and business telephone number of an affiliate of the custodian who can answer the individual's questions about the collection.

The requirement to provide notification applies only in those situations where information is collected directly from an individual such as on an application, admission or intake form or on a client survey.

"Purpose of collection" means the reason for which the information is needed and the use(s) that the custodian will make of that information.

"Legal authority for collection" refers to the statute or regulation of Alberta or Canada that expressly authorizes collection of the information, or **section 20(b)** which authorizes collection of individually identifying health information if that information relates directly to and is necessary to enable the custodian to carry out a purpose that is authorized under **section 27**.

Identifying someone to answer an individual's questions about the collection is intended to provide the individual with a knowledgeable source of information. The person or position cited should be familiar with the program and be able to explain why the information is being collected and how it will be used and retained by the custodian and how it may be disclosed to other custodians or non-custodians, if that is required or permitted.

The requirement to notify recognizes the individual's right to know and understand the purpose of the collection of individually identifying health information and how the information will be used. It also allows the individual to make an informed decision as to whether to give the information when there is no statutory requirement to do so.

The notice may be given by:

- printing it on a collection form;
- putting it on a separate sheet or in a brochure accompanying the form;
- publishing it in an information brochure about a program;
- displaying it on a notice hung on the wall or placed on a service counter; or
- giving it verbally.

The same form of notice is required for computer-generated forms, regardless of whether a custodian or an affiliate enters the information about the individual or the individual does the entry.

The notice must contain all three elements in **section 22(3).** It should be given to the individual at the beginning of an interview or brought to an applicant's attention before the applicant begins to fill out an application form. If the interview is being recorded, it is good practice to record the notice at the beginning of the tape.

When individuals are applying for and participating in extensive and complementary programs, it may be more convenient and effective to place a generic notice in a publication about the program or to explain this orally. In a physician's office or at a community pharmacy, collection notices could be posted on a wall or handed to a patient or client at the reception area or counter.

However, it is important that the individual have an opportunity to make an informed decision as to whether to give the information and understand any consequences that may result from not doing so. This applies as well when information is collected over the telephone.

When notice is given verbally, either in person or over the telephone, the custodian should ensure that the individual is informed of the privacy requirements in the *Act*. An explanatory document can be provided either at the counter or later by mail. It is also a good practice to provide written confirmation of telephone collection of personal information.

Where practicable, the custodian should provide an applicant with a copy of the notice and retain a copy on file.

BEST PRACTICES: *As part of the review of information practices and assessing compliance with the provisions of the Act, custodians should regularly review their collection instruments (forms) to determine which ones require collection notices.*

Custodians should ensure that individuals are not misled as to the purpose of a collection and that they have not been threatened or coerced during the collection process. If an individual is uncomfortable with one way of collecting information, custodians should find another way of collecting the information if that is possible. Individuals should not be asked intimate questions that are not necessary for the purpose (e.g. treatment or diagnosis). Custodians should make an effort to ensure that verbal collection is conducted in such a way that the information cannot be overheard by other clients or patients.

6.7 USING A RECORDING DEVICE

In certain cases, information about an individual may be collected by using a recording device, camera or other device that may not be obvious to the individual. This could include cases where a health services provider is observing an individual in a certain therapy or treatment session.

Section 23 says that a custodian that collects health information from an individual using a recording device or camera or any other device that may not be obvious to the individual must, before collecting the information, obtain the written consent of the individual for the of the device or camera.

Consent to use a recording device could be given by a representative of the individual under **section 104(1)**.

THINGS TO REMEMBER

COLLECTION OF HEALTH INFORMATION

- A custodian must not collect health information except in accordance with the *Health Information Act.*
- A custodian may collect non-identifying health information for any purpose.
- An affiliate must only collect the health information that is necessary for that affiliate to carry out his/her responsibilities as assigned by the custodian.
- A custodian must collect the least amount of health information at the highest level of anonymity possible unless the collection is for providing a health service or determining the eligibility of an individual to receive a health service.
- A custodian may only collect individually identifying health information if the collection is expressly authorized by an enactment of Alberta or Canada or if the information relates directly to and is necessary to enable the custodian to carry out an authorized purpose under section 27 of the *Health Information Act* (see the list of authorized purposes under 'Use of Health Information' – Chapter 7 of this Publication).
- A custodian must collect individually identifying health information directly from the individual who is the subject of the information, unless indirect collection is authorized under the *Act*.
- A custodian may collect individually identifying health information indirectly (from a person other than the individual it is about) where:
    - the individual authorizes collection from someone else;
    - the individual is unable to provide the information and the information is collected from the individual's authorized representative;
    - direct collection would prejudice the interests of the individual, the purposes of collection or the safety of another individual;

  - collection is for the purpose of assembling a family or genetic history needed to provide a health service to the individual;
  - collection is for the purpose of determining or verifying the individual's eligibility to participate in a program or receive a benefit;
  - collection is for the purpose of informing the Public Trustee or Public Guardian about clients or potential clients;
  - the information is available to the public; or
  - disclosure is authorized under Part 5 of the *Act* (Disclosure of Health Information).

- When collecting individually identifying health information directly from the individual it is about, a custodian must take reasonable steps to inform the individual about:

  - the purpose for collection;
  - the legal authority for the collection; and
  - the title, business address and business telephone number of an affiliate who can answer questions about the collection. (See the Sample Collection Notice in Appendix 1 of the Manual).

- A custodian must obtain the consent of the individual or an authorized representative before collecting health information using a recording device or camera that is not obvious to the individual.

Collection of Personal Health Numbers

- Only a custodian and persons authorized by section 5 of the Health Information Regulation have the right to require an individual to provide their personal health number.

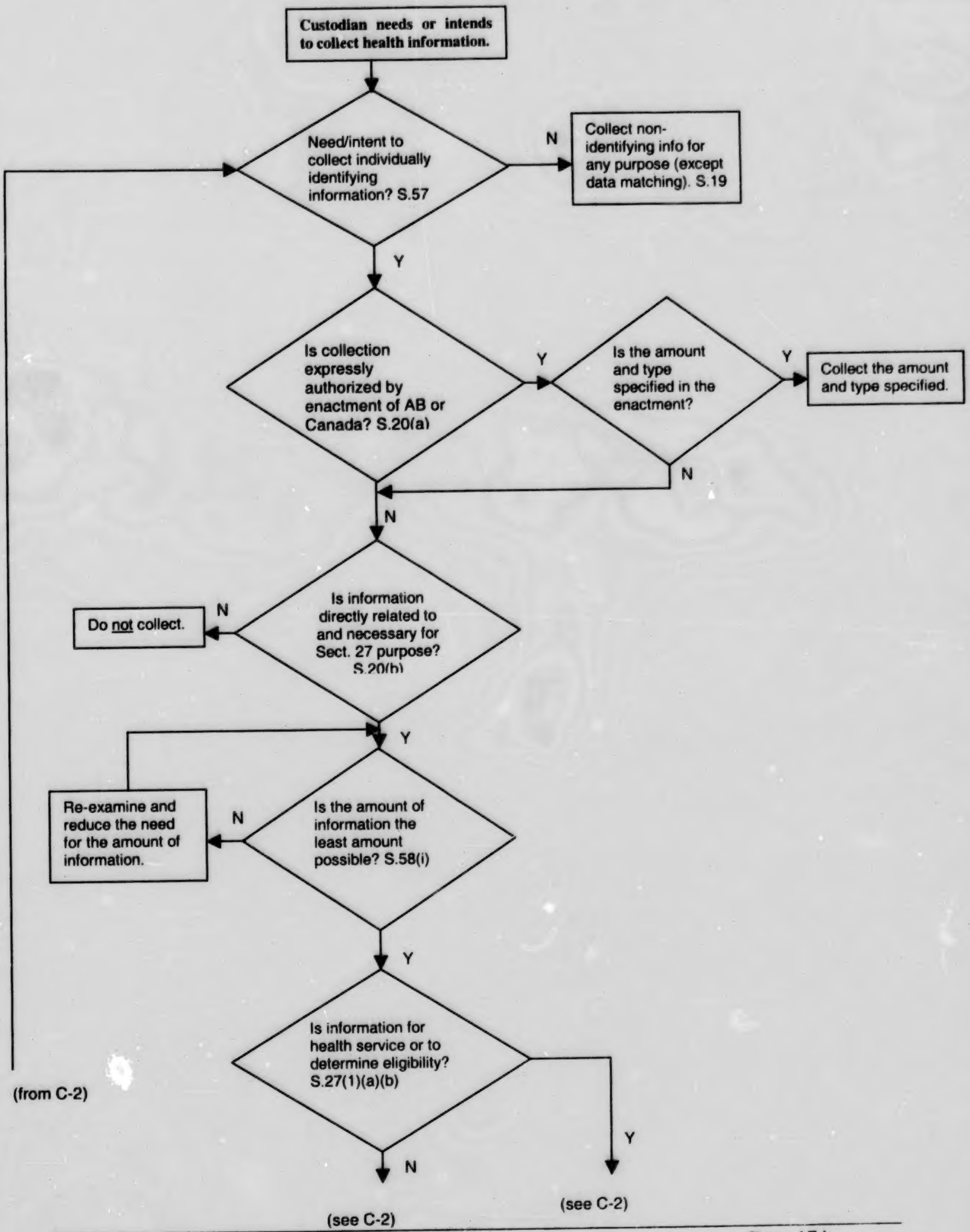
- A custodian and a person listed in section 5 of the Health Information Regulation must advise individuals of their authority to collect personal health numbers before they request the number from the individual.

- An individual can refuse to provide their personal health number to someone other than a custodian or a person listed in section 5 of the Health Information Regulation.

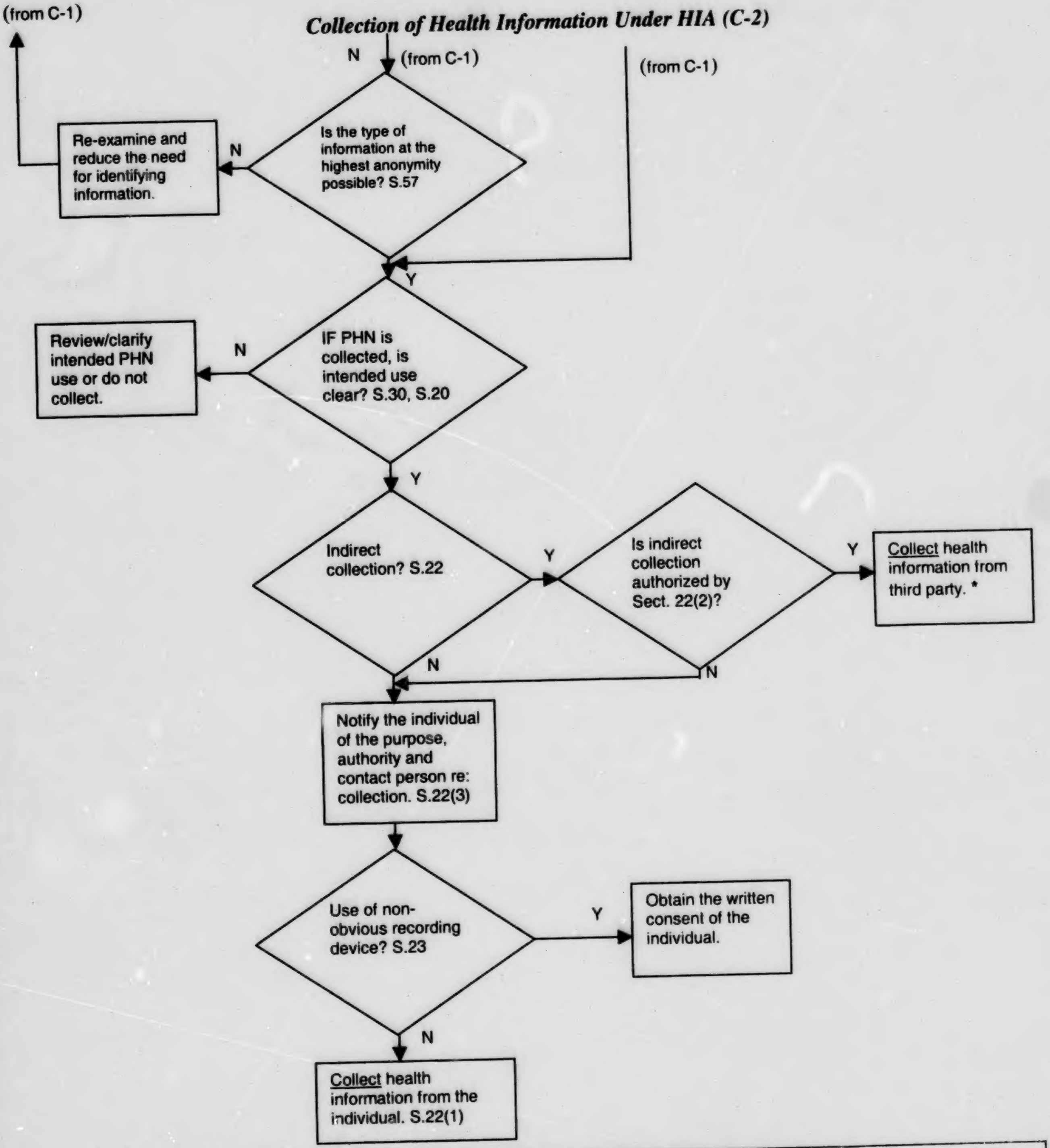
Besides Custodians, Who Can Require Individuals to Provide their Personal Health Numbers?
(Section 5 of the Health Information Regulation)

- the Students Finance Board to administer student health benefits programs;
- lawyers and insurers for the purpose of enforcing the Crown's right of recovery under Part 5 of the *Hospitals Act;*
- an Insurer (ABC Benefits Corporation or an insurer licensed under the *Insurance Act)* to handle, assess and pay benefit claims;
- the Workers' Compensation Board to handle, assess and pay benefit claims;
- ambulance attendants and operators under the *Ambulance Services Act* to provide health services and seek reimbursement from Alberta Blue Cross;
- the Minister of Justice and Attorney General to provide health services to an inmate outside of a correctional institution;
- the Minister of Community Development to administer the *Senior's Benefit Act*;
- the Minister of Human Resources and Employment to administer income and employment programs of that department; and
- persons other than custodians who provide health services to enable them to seek reimbursement for those services from the Alberta Health Care Insurance Plan.

Collection of Health Information Under HIA (C-1)


Custodian needs or intends to collect health information.
Need/intent to collect individually identifying information? S.57
N
Collect non-identifying info for any purpose (except data matching). S.19
Y
Is collection expressly authorized by enactment of AB or Canada? S.20(a)
Y
Is the amount and type specified in the enactment?
Y
Collect the amount and type specified.
N
N
Is information directly related to and necessary for Sect. 27 purpose? S.20(b)
N
Do not collect.
Y
Is the amount of information the least amount possible? S.58(i)
N
Re-examine and reduce the need for the amount of information.
Y
Is information for health service or to determine eligibility? S.27(1)(a)(b)
(from C-2)
Y
N
(see C-2)
(see C-2)

Collection of Health Information Under HIA (C-2)


(from C-1)
N
(from C-1)
(from C-1)
Re-examine and reduce the need for identifying information.
N
Is the type of information at the highest anonymity possible? S.57
Y
Review/clarify intended PHN use or do not collect.
N
IF PHN is collected, is intended use clear? S.30, S.20
Y
Indirect collection? S.22
Y
Is indirect collection authorized by Sect. 22(2)?
Y
Collect health information from third party. *
N
N
Notify the individual of the purpose, authority and contact person re: collection. S.22(3)
Use of non-obvious recording device? S.23
Y
Obtain the written consent of the individual.
N
Collect health information from the individual. S.22(1)

* Note – If collection is from a custodian under the *Health Information Act*, that custodian may disclose the information only in accordance with the disclosure rules of the *Act*.

CHAPTER SEVEN

USE OF HEALTH INFORMATION

7.1 OVERVIEW OF CHAPTER SEVEN

This chapter will cover:

- the limits on the use of health information;
- the duties of custodians using health information;
- the use of non-identifying health information;
- the authority for custodians to use individually identifying health information;
- the application of the 'need to know' principle to the use of health information by affiliates;
- the limits on the use of non-recorded health information; and
- the use of personal health number by non-custodians authorized by regulation.

7.2 LIMITS ON THE USE OF HEALTH INFORMATION

The rules governing the use of health information are found in **Part 4** of the *Act* **(Use of Health Information) (sections 25 to 30)** and also within the duties of custodians relating to health information in **Part 6** of the *Act* **(sections 57 and 58)**.

"Use" means applying health information for a purpose and includes reproducing the information, but does not include disclosing the information **(section 1(1)(w))**.

A custodian may use individually identifying health information for such things as providing health services; determining an individual's eligibility for a program or benefit; providing for health services provider education; carrying out an authorized purpose under an enactment of Alberta or Canada; for internal management purposes and other specified uses **(section 27(1))**.

The concept of use also includes appropriate and controlled access to and sharing of health information within a custodian. This means that if a custodian needs to carry out an authorized purpose under **section 27** by sharing individually identifying health information within the scope of the custodian (e.g. a hospital within a regional health authority sharing health information with other hospitals within the region for the purposes of continuing treatment and care of an individual or for health system management), this would be a **"use"** of the information, not a **"disclosure"** under the *Act*.

Custodians are bound by the requirements of the *Act* whether the use of the information is carried out by the custodian or by its affiliates.

There are a number of limitations on use of health information in the *Act*, particularly those related to the use of individually identifying health information and also to the use of personal health numbers. Individually identifying health information can only be used under the conditions set out in the *Act*. However, these rules do not apply to the use of health information that does not reveal the identity of individuals (non-identifying health information).

A general prohibition on the use of health information is set out in **section 25.** That section says that custodians must not use health information except in accordance with the *Act*.

Recipients of health information must not:

- use the information for direct commercial marketing or fundraising purposes without consent **(section 107(2)(f))**;
- take steps to re-identify an individual from non-identifying health information through data matching without first notifying the Information and Privacy Commissioner **(section 32(2))**; or
- require an individual to provide their personal health number unless they have that authority under **section 21 or section 5(2)** of the Health Information Regulation and must not use the number for any additional purpose.

7.2.1 DUTY TO USE HEALTH INFORMATION WITH THE HIGHEST DEGREE OF ANONYMITY POSSIBLE

Custodians using health information must consider the level of anonymity that is needed for the intended purpose. They must first consider whether the use of aggregate health information will be adequate for the intended purpose and if so, must only use aggregate health information **(section 57(2))**.

"Aggregate health information" is defined in **section 57(1)** to mean non-identifying health information about groups of individuals.

If the custodian believes that using aggregate health information will not be adequate for the custodian's intended purpose, the custodian must then consider whether use of other non-identifying health information is adequate for the intended purpose, and if so, the custodian must use the other non-identifying health information **(section 57(3))**.

"Non-identifying health information" is defined in **section 1(1)(r)** to mean that the identity of the individual who is the subject of the information cannot be readily ascertained from the information.

Under **section 57(4),** if the custodian believes that using aggregate and other non-identifying health information will not be adequate for the custodian's intended purpose, the custodian may use individually identifying health information if the use is:

- authorized by the *Health Information Act;* and
- carried out in accordance with the *Health Information Act.*

Under **section 65**, a custodian may strip, encode or otherwise transform individually identifying health information to create non-identifying health information.

"Individually identifying health information" is defined in **section 1(1)(q)** to mean that the identity of the individual who is the subject of the information can be readily ascertained from the information.

"Readily ascertained" in the context of **section 57,** means that the identity of an individual (e.g. the individual's name or other identifiers or distinguishing characteristics associated with an individual) can be determined or deduced without having to apply a sophisticated technical method or process, or without having the particular technical expertise to do so. An individual's identity can be said to be "readily ascertained" if his or her identity can be determined by:

- combining available information within the same or in several different records;
- comparing information representing distinguishing characteristics with other information sources having both the distinguishing characteristics and the names or other identifiers of individuals; and
- if only readily available or conventional computer hardware, software and technical expertise is used.

Section 57 does not apply where the use of health information is for the purpose of providing a health service (as defined in **section 1(1)(m)**), or for determining the eligibility of an individual to receive a health service.

See section 5.3.1 of Chapter 5 of this Publication for a more detailed discussion of this duty.

7.2.2 DUTY TO USE HEALTH INFORMATION IN A LIMITED MANNER

In addition to complying with **section 57**, custodians must only use the amount of health information that is essential to enable the custodian to carry out the intended purpose **(section 58(1))**.

See section 5.2.2 of Chapter 5 of this Publication for a more detailed discussion of this duty.

7.2.3 APPLYING THE 'NEED TO KNOW' PRINCIPLE TO THE USE OF HEALTH INFORMATION BY AFFILIATES

Just as the *Act* limits the authority of affiliates to collect health information, it also limits the authority of affiliates to use health information. Under **section 28**, an affiliate of a custodian must not use health information in any manner that is not in accordance with the affiliate's duties to the custodian.

This means that unless the information is necessary for the affiliate to carry out one of its/his/her designated responsibilities, the affiliate should not be using that information. This also implies that custodians must identify the roles and responsibilities of their affiliates and ensure that affiliates are informed about their duties and responsibilities. These roles and responsibilities will limit the amount and the level of anonymity of health information they will need to use.

In the context of a hospital setting, those affiliates who are directly involved with assessment, diagnosis, treatment and care of an individual would need to use individually identifying diagnostic, treatment and care information about the individual. They would also likely need access to the most complete health information about the individual to ensure that all relevant information is taken into account.

Other care providers such as pharmacy and dietary personnel may require certain individually identifying information to carry out their duties and responsibilities but in most cases, would not need access to the complete file for all patients.

In a multi-unit facility, affiliates working in one unit are usually not involved in the care of patients in another unit, unless they are covering off in the event of staff shortages or in an emergency. Except in those cases, they would therefore not need to know or use health information about the patients for whom they are not providing care or health services.

7.2.4 LIMITS ON THE USE OF NON-RECORDED HEALTH INFORMATION

While the *Act* applies primarily to health information that is written or otherwise recorded and stored, it also places a duty on custodians and their affiliates to protect the confidentiality of information that is not recorded.

"Confidentiality" implies a trust relationship between the person supplying information and the individual or organization collecting it. The relationship is built on the assurance that the information will only be used by or disclosed to authorized persons or to others with the individual's permission.

Section 29 states that a custodian that collects diagnostic, treatment and care information (as defined in **section 1(1)(i)**), health services provider information (as defined in **section 1(1)(o)**), or registration information (as defined in **section 1(1)(u)**) that is not written, recorded or stored in some manner in a record may use the information only for the purpose for which the information was provided to the custodian.

This means that if a custodian or its affiliates collect or become aware of the above types of information related to an individual but the information is not recorded, it can still only be used for the purpose for which it was collected.

7.3 USING NON-IDENTIFYING HEALTH INFORMATION

Custodians may use non-identifying health information for any purpose (**section 26**). Practically speaking, health information is really only non-identifying information if the custodian or other person or entity receiving the information does not have other information that could, in combination, identify an individual.

7.4 AUTHORITY FOR CUSTODIANS TO USE INDIVIDUALLY IDENTIFYING HEALTH INFORMATION

Custodians who are health service providers rely on the controlled use of health information. Their ability to use individually identifying health information is essential to the provision of continuing care and treatment to an individual. For example, specialists, nurses, other health professionals and home care workers need to use health information about an individual collected from the individual's family physician. Pharmacists need to use information about an individual's allergies as well as other medications that the individual may be taking before filling their prescriptions or advising them about over-the- counter medications.

Within a hospital setting, health service providers work together to provide the best treatment and care to a patient, often using health information that has been collected by another provider.

Custodians also need to use individually identifying health information for such things as conducting investigations, discipline proceedings or practice reviews relating to a member of a health profession or health discipline; providing for health services provider education; conducting research under certain conditions; or for internal management purposes.

7.4.1 AUTHORIZED PURPOSES

Section 27(1) sets out the situations in which an individual's health information may be used by a custodian. This section states that a custodian may use individually identifying health information in its custody or under its control for certain authorized purposes.

The information in the custody or under the control of a custodian may have been collected directly from the individual it is about or indirectly from other sources (with authority) or it could have been compiled by the custodian (i.e. drawn from several sources with a new set of information created).

The line between use and disclosure of health information is sometimes difficult to detect. The movement of health information within the sphere of influence of a custodian e.g. to various sites within a regional health authority, or to an affiliate of that custodian (an employee, contractor, agent or volunteer) is a **use** of the information. However, the movement of health information between custodians or outside the sphere of influence of a custodian is a **disclosure** of the information.

For example, movement of health information between a regional health authority and an approved hospital (as defined in the *Hospitals Act*), other than one that is owned by the regional health authority, would be a disclosure of individually identifying health information. However, if the approved hospital provided laboratory services to the health authority under a contract, the approved hospital would be using, not disclosing the health information.

See section 2.3 in Chapter 2 of this Publication for definitions of "custody" and "control".

The authorized purposes are:

- providing health services **(section 27(1)(a));**

  Examples of this would be doctors, nurses and other health services providers reviewing an individual's chart or file so that they can make a diagnosis or provide a health service.

  A **"health service"** is defined in **section 1(1)(m).**

  See section 1.4.1 of Chapter 1 of this Publication for a more detailed discussion of what is and is not included in a "health service".

- determining or verifying the eligibility of an individual to receive a health service **(section 27(1)(b));**

  This use would enable a custodian to check to see if a person is registered for Alberta Health Care Insurance or other benefits or to assess whether an individual meets the eligibility criteria for example, the Alberta Aids to Daily Living Program.

- conducting investigations, discipline proceedings, practice reviews or inspections relating to the members of a health profession or health discipline **(section 27(1)(c))**;

Under this provision, individually identifying health information could be used by a custodian to investigate the actions or conduct of, or to initiate disciplinary action against, an employee, contractor or agent who is a member of a health profession or health discipline.

"Health profession" refers to the professions that are included in the *Health Professions Act (when proclaimed in force for the particular profession)* e.g. physicians, nurses, physiotherapists, psychologists, medical laboratory technologists, midwives.

"Health discipline" refers to the professions or occupations that are included in the *Health Disciplines Act* e.g. psychiatric nurses, licensed practical nurses, acupuncturists.

"Investigation" refers to a systematic process of examination, inquiry and observation.

"Discipline proceeding" refers to a formal process of determining whether a practitioner has displayed a lack of skill or judgment in the practice of his or her profession; has displayed unbecoming and/or unprofessional, disgraceful or dishonourable conduct; or is incapable or unfit to practice his or her profession.

"Practice review" refers to an assessment or evaluation of the professional performance or competence of a practitioner.

"Inspection" refers to the examination or viewing of the physical premises or of the books, records, papers or other documents of a practitioner as part of an investigation.

- conducting research;
  - if the custodian has submitted a proposal to an ethics committee in accordance with **section 49**;
  - if the ethics committee is satisfied as to the matters referred to in **section 50(1)(b)**;
  - if the custodian has complied with or undertaken to comply with the conditions, if any, suggested by the ethics committee; and
  - where the ethics committee recommends that consents should be obtained from the individuals who are the subjects of the health information to be used in the research, if those consents have been obtained **(section 27(1)(d))**;

Individually identifying health information may be used by a custodian, without an individual's consent, for conducting research only if this has first been approved by an ethics committee and if the researcher complies with **sections 49 and 50(1)(b)** and any conditions set by the ethics committee.

Individually identifying health information may be needed so researchers employed by or under contract to a custodian can assess the outcomes of certain treatments or benefit programs.

"Research" is defined in **section 1(1)(v)** as academic, applied or scientific health-related research that necessitates the use of individually identifying diagnostic, treatment and care information or individually identifying registration information, or both.

This definition does not include the use of individually identifying health services provider information for research purposes.

An **"ethics committee"** means a committee designated by the regulations as an ethics committee **(section 1(1)(j))**. **Section 2** of the Designation Regulation lists the committees and boards that have been designated as ethics committees for the purposes of **Division 3 of Part 5 (Disclosure for Research Purposes)**. Examples are: University of Calgary Conjoint Health Research Ethics Board; College of Physicians and Surgeons of Alberta – Research Ethics Review Board; and Alberta Cancer Board – Research Ethics Committee.

See section 8.15 of Chapter 8 of this Publication for more discussion of sections 48-56 dealing with Disclosure for Research Purposes.

- providing for health services provider education **(section 27(1)(e))**;

This provision enables a custodian to use individually identifying health information to train health services providers through case studies, grand rounds, in-service education, etc. However, this use must still respect the principle of highest level of anonymity possible. It may not be necessary, for example, to use individually identifying health information in a case study presented in a non-clinical context.

"Health services provider" means an individual who provides health services **(section 1(1)(n))**.

- carrying out any purpose authorized by an enactment of Alberta or Canada **(section 27(1)(f))**;

An **"enactment"** could be a statute or a regulation under a statute. Other statutes that authorize the use of individually identifying health information include the ***Regional Health Authorities Act***, the ***Hospitals Act***, the ***Public Health Act*** and the ***Mental Health Act***.

- and for internal management purposes, including planning, resource allocation, policy development, quality improvement, monitoring, audit, evaluation, reporting, obtaining or processing payment for services and human resource management **(section 27(1)(g))**.

When custodians require non-identifying information for these secondary, internal management purposes, they may convert individually identifying health information into non-identifying form. The non-identifying health information is usually sufficient to achieve the intended purpose, although at times, individually identifying health information may be required. It may be necessary, for example, for a custodian to verify information, assess compliance, coordinate services to individuals or track services to individuals across different jurisdictions.

Custodians may create non-identifying information by grouping it (i.e. aggregating it) or by stripping the identifiers to create individual anonymous information. If a custodian intends to use non-identifying health information, it may be necessary for the custodian to retain identifiers for data-matching processes. The custodian can strip the identifiers for the final disclosure/use of the information once the data match has been made.

Section 27(1)(g) authorizes these kinds of uses of individually identifying health information.

Examples of uses for internal management are:

"planning" – projecting expected service demands to determine what resources will be needed for the future (e.g. capital resources, human resources, equipment, supplies, etc.);

"resource allocation" –examining current service demand to allocate resources where they can be best used (e.g. allocating human resources to different wards and shifts);

"policy development" – examining patient/population needs to determine what new policies and programs may be required;

"quality improvement" – examining existing services and patient outcomes to determine how services can be improved for the future;

"monitoring" – monitoring services provided to ensure that affiliates are accountable for their activities and the resources they use;

"auditing" – auditing clinical records to ensure that record keeping by affiliates meets legislated requirements. May also need to audit financial records for accountability purposes;

"Audit" means a financial, clinical or other formal or systematic examination or review of a program, portion of a program or activity **(section 1(1)(c))**;

"evaluation" – evaluating services to ensure they are being delivered appropriately and efficiently;

"reporting, obtaining or processing payment for services" – billing funding sources for services provided to patients (e.g. billing Alberta Health Care Insurance Plan, private insurance plans, patients directly); and

"human resource management" – monitoring affiliates' conduct and competence, including reporting concerns about the conduct and competence of professionals to their respective regulatory bodies; may also need to undertake workload measurements to determine what human resources are required (mix and quantity).

Note: this use does not cover a custodian using patient files for the human resource management of its staff who may also be its patients. This health information cannot be used for selection, appraisal or termination of a member of a custodian's staff.

7.4.2 ADDITIONAL AUTHORIZED PURPOSES FOR CUSTODIANS WITH HEALTH SYSTEM MANDATES

Section 27(2) authorizes certain custodians with health system management responsibilities to use individually identifying health information for all of the purposes in **27(1)** and also for four additional purposes.

The custodians that may use individually identifying health information for these additional health system purposes are:

- a provincial health board (i.e. Alberta Mental Health Board) established pursuant to regulations made under **section 17(1)(a)** of the *Regional Health Authorities Act* **(section 1(1)(f)(iii))**;
- a regional health authority established under the *Regional Health Authorities Act* **(section 1(1)(f)(iv))**;
- the Alberta Cancer Board continued under the *Cancer Programs Act* **(section 1(1)(f)(vii))**;
- the department **(section 1(1)(f)(xii))**; and
- the Minister**(section 1(1)(f)(xiii))**.

These custodians are created, funded and held accountable for certain functions (including those listed in **section 27(2)**) within their assigned mandate. In order to carry out these functions, they may need to use individually identifying health information in certain limited situations. In these cases, individually identifying information is often combined or aggregated to develop anonymous information about groups of individuals.

The main difference between health system purposes and internal management purposes is that health system purposes often require information to be collected from several custodians to undertake the purpose.

Non-identifying health information is usually sufficient to achieve these purposes but at times, individually identifying health information may be required. The general rules in the *Act* to collect, use and disclose the least amount of information, at the highest degree of anonymity apply to these custodians when undertaking health system purposes. While individually identifying health information may be needed in the original data collection or manipulation stages of the process, in most instances, the information could and should be aggregated and/or anonymized prior to completing all of the process steps necessary to achieve the purpose.

These additional or secondary authorized purposes for the above custodians are:

- **planning and resource allocation (section 27(2)(a))**;

  The Minister may use individually identifying health information for planning and resource allocation at the provincial, regional and program levels. Health authorities may use this type of health information for planning and resource allocation at the regional, program, facility and unit levels.

  For example, the provincial costing project calculates Alberta-based costs for various types of health services for funding projections. Business cases are built for allocating resources across different clinical programs. Future expenditures are forecast at the provincial or regional program levels. Health authorities need to plan for the costs of providing certain treatments such as dialysis or home intravenous treatments.

- **health system management (section 27(2)(b));**

  This enables the Minister to use individually identifying health information for this purpose at the provincial, regional and program levels. It enables health authorities to use it for health system management at the regional and program levels.

  Examples are:
  - analyzing the incidence of illness or contributing factors leading to an illness or disease to introduce new health promotion or prevention programs;
  - enabling the Minister to administer the third party liability program (tracking costs for services provided to individuals and seeking reimbursement from the liable parties);
  - coordinating health benefits with the Workers' Compensation Board, the federal health programs (for RCMP, aboriginals), etc; and
  - managing drug programs; verifying the need for capital construction plans; managing health programs (e.g. physical therapy, home care).

- **public health surveillance (section 27(2)(c));**

  This function includes the use of individually identifying health information for the surveillance of infectious diseases and environmental hazards under the *Public Health Act* and detecting cancer and other diseases.

  Examples are:
  - reporting individual cases of and contact tracing for communicable diseases;
  - assessing environmental health hazards;
  - screening programs to identify and track individuals (for breast cancer screening, newborn metabolic screening, cervical cancer screening, HIV and Hepatitis B prenatal screening); and
  - immunization programs.

- **health policy development (27)(2)(d);**

  Health policy development needs to be based on an accurate picture of current health needs or health service delivery practices, but health policy decision makers would not need to know the names and individual health details of each person in the affected population. Individual identifiers should be removed as early as possible in the process.

  Examples are:
  - tracking services to specific individuals so services can be coordinated across jurisdictions (regions, government departments, provinces);
  - developing future programs for specific target groups (e.g. aboriginals, children, seniors, etc.);
  - developing policy from utilization analysis of programs and treatments; and
  - developing new alternative payment plans for physicians.

7.5 USE OF PERSONAL HEALTH NUMBER BY PERSONS AUTHORIZED BY REGULATION

Section 30 states that a person who has the authority to require an individual to provide a personal health number pursuant to **section 21(1)(b)** may use the information only for the purpose for which the information was collected.

See **section 5(2)** of the Health Information Regulation for a list of the persons and organizations that can require an individual to provide his or her personal health number.

The restriction on the use of personal health numbers is necessary because the PHN creates a single point of access to a large amount of identifying health information about an individual and therefore represents a single point of risk for unauthorized access or misuse of this information.

See also section 6.5.1 in Chapter 6 of this Publication for a discussion on collection of personal health numbers.

THINGS TO REMEMBER

USE OF HEALTH INFORMATION

- A custodian must not use health information except in accordance with the *Act*.
- "Use" includes having access to or sharing health information between affiliates of the custodian.
- A custodian may use non-identifying health information for any purpose.
- A custodian may only use individually identifying health information for the authorized purposes under section 27.
- A person authorized to require an individual to provide a personal health number (under section 21(1)(b)) may only use that number for the purpose for which it was collected.
- A custodian may only use non-recorded individually identifying health information for the purpose for which the information was provided to the custodian.
- A custodian must use the least amount of health information at the highest level of anonymity possible unless it is being used for the purpose of providing a health service or for determining the eligibility of an individual to receive a health service.
- An affiliate must not use health information unless it is necessary to enable the affiliate to carry out his/her/its responsibilities as assigned by the custodian.

AUTHORIZED PURPOSES
SECTION 27(1)

A custodian may use individually identifying health information in its custody or under its control for the following authorized purposes:

- Providing health services;
- Determining or verifying the eligibility of an individual to receive a health service;
- Conducting investigations, discipline proceedings, practice reviews or inspections relating to the members of a health profession or health discipline;
- Conducting research if:
  - the custodian has submitted a proposal to an ethics committee in accordance with section 49;
  - the ethics committee is satisfied as to the matters in section 50(1)(b);
  - the custodian has complied with or agreed to comply with the conditions suggested by the ethics committee; and
  - consents have been obtained where recommended by the ethics committee;
- Providing for health services provider education;
- Carrying out any purpose authorized by an enactment of Alberta or Canada; and
- For internal management purposes, including planning, resource allocation, policy development, quality improvement, monitoring, audit, evaluation, reporting, obtaining or processing payment for services and human resource management.

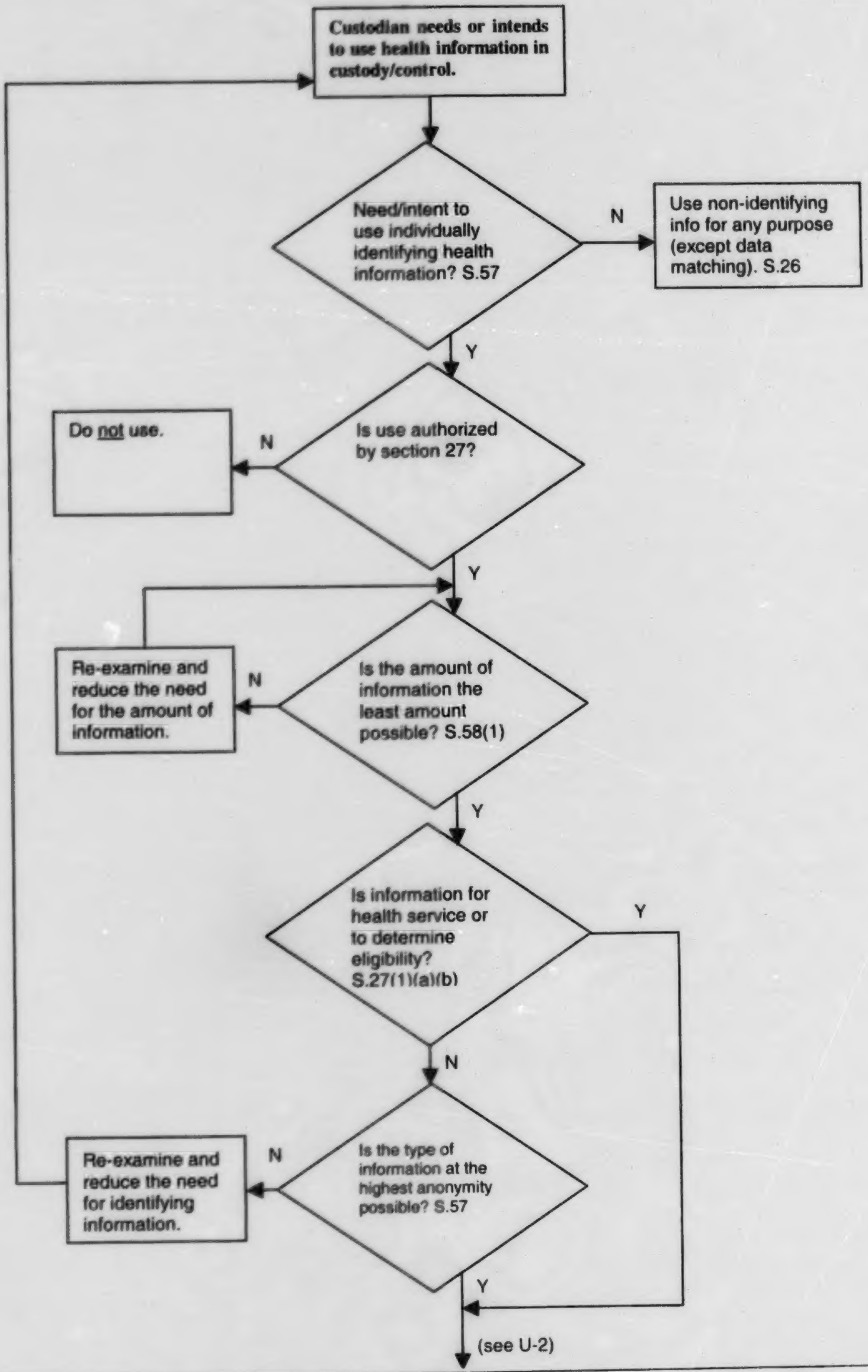
AUTHORIZED PURPOSES
SECTION 27(2)

In addition to the authorized purposes in section 27(1) of the *Act*, regional health authorities, the Alberta Cancer Board, the Alberta Mental Health Board, the Department and the Minister may also use individually identifying health information in their custody or under their control to carry out the following functions within the geographic area in which the

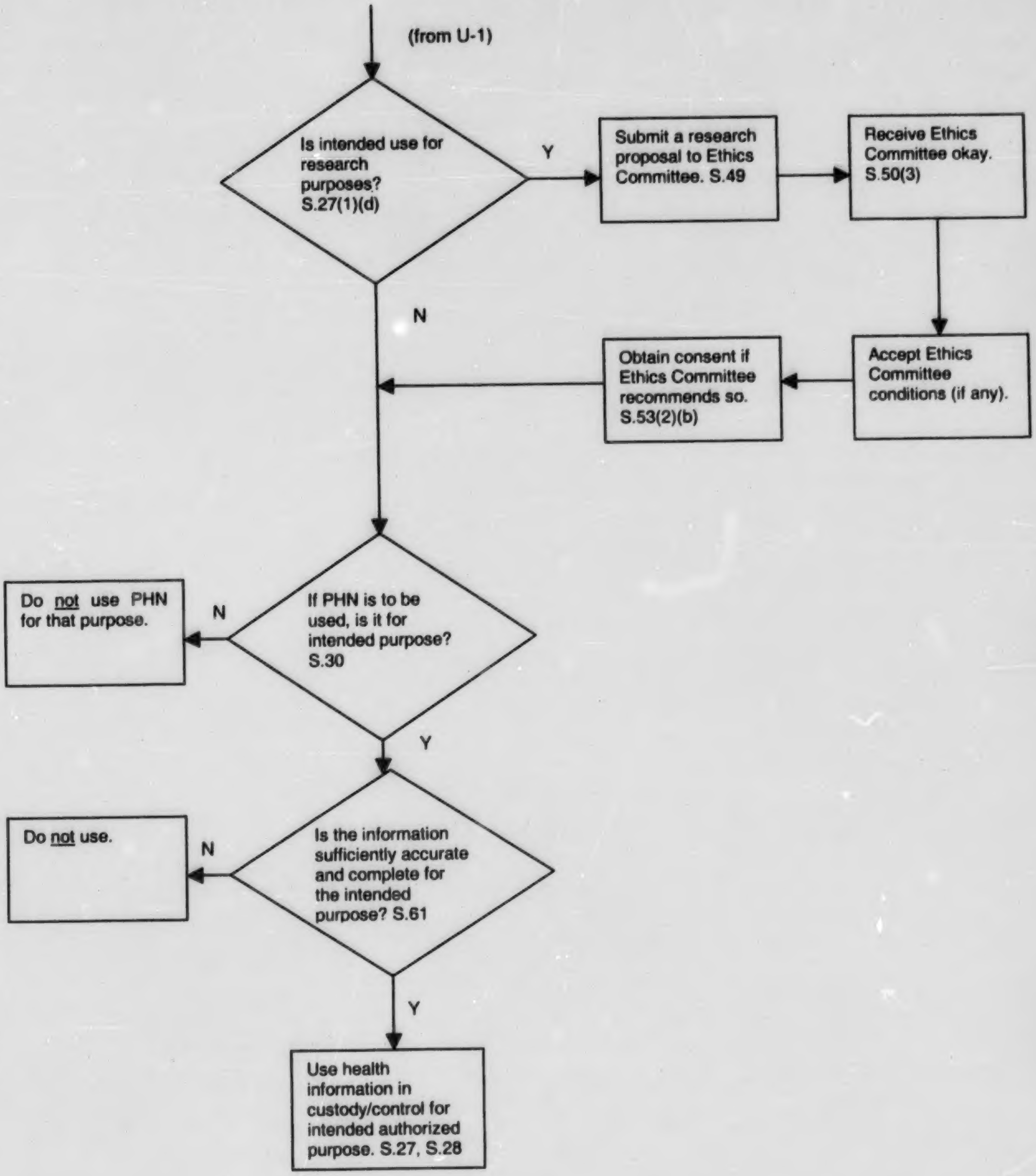
custodian has jurisdiction to promote the objectives for which the custodian is responsible:

- Planning and resource allocation;
- Health system management;
- Public health surveillance; and
- Health policy development.

Use of Health Information Under HIA (U-1)


Custodian needs or intends to use health information in custody/control.
Need/intent to use individually identifying health information? S.57
N
Use non-identifying info for any purpose (except data matching). S.26
Y
Is use authorized by section 27?
N
Do not use.
Y
Is the amount of information the least amount possible? S.58(1)
N
Re-examine and reduce the need for the amount of information.
Y
Is information for health service or to determine eligibility? S.27(1)(a)(b)
Y
N
Is the type of information at the highest anonymity possible? S.57
N
Re-examine and reduce the need for identifying information.
Y
(see U-2)

Use of Health Information Under HIA (U-2)


(from U-1)
Is intended use for research purposes? S.27(1)(d)
Y
Submit a research proposal to Ethics Committee. S.49
Receive Ethics Committee okay. S.50(3)
Accept Ethics Committee conditions (if any).
Obtain consent if Ethics Committee recommends so. S.53(2)(b)
N
If PHN is to be used, is it for intended purpose? S.30
N
Do not use PHN for that purpose.
Y
Is the information sufficiently accurate and complete for the intended purpose? S.61
N
Do not use.
Y
Use health information in custody/control for intended authorized purpose. S.27, S.28

CHAPTER EIGHT

DISCLOSURE OF HEALTH INFORMATION

8.1 OVERVIEW OF CHAPTER EIGHT

This Chapter will cover:

- the limits on disclosure of health information;
- the duties of custodians and affiliates regarding the disclosure of health information;
- the disclosure of non-identifying health information;
- disclosure of individually identifying health information with consent;
- disclosure of diagnostic, treatment and care information without consent;
- notification of recipients of the purpose and authority for disclosure of diagnostic, treatment and care information;
- disclosure of diagnostic, treatment and care information by electronic means;
- maintenance of information on disclosures of individually identifying diagnostic, treatment and care information;
- disclosure of registration information without consent;
- disclosure of health services provider information without consent;
- disclosure of individually identifying health information without consent to archives;
- disclosure of individually identifying health information to the Minister without consent;
- disclosure of individually identifying health information by the Minister and department;
- disclosure to Minister or department or to certain other custodians for health system purposes; and
- disclosure for research purposes.

8.2 LIMITS ON DISCLOSURE OF HEALTH INFORMATION

The rules governing the disclosure of health information are found in **Part 5** of the *Act* **(sections 31-56)** and also within the duties of custodians relating to health information in **Part 6** of the *Act* **(sections 57 and 58)**. These rules refer to the provision of health information to someone other than the individual that it is about, usually to a third party. They attempt to balance the protection of individual privacy with the disclosure of health information.

Although **"disclosure"** is not defined in the *Act*, the definition of **"use"** in the *Act* **(section 1(1) (w))** does not include the disclosure of health information. If a hospital within a regional health authority shares health information with hospitals within the region for an authorized purpose under **section 27**, it would be **"using"** health information, not **"disclosing"** it. This is consistent with **section 62(2)**. Under that section, any collection, use or disclosure of health information by an affiliate of a custodian is considered to be collection, use or disclosure by the custodian.

"Disclosure" refers to the release, transmittal, exposure, revealing, showing, providing copies of, telling the contents of, or giving health information by any means to any person or organization. It includes disclosure to another custodian or to a non-custodian.

It includes oral transmission by telephone, voice mail or in person; provision of the information on paper, by facsimile or in another format; and electronic transmission through electronic mail, data transfer or the Internet.

A general prohibition on the disclosure of health information is set out in **section 31**. That section says that custodians must not disclose health information except in accordance with the *Act*.

Custodians are bound by the requirements of the *Act* whether the disclosure of the information is carried out by the custodian or by its affiliates.

Individually identifying health information can only be disclosed in accordance with the rules set out in the *Act*. Those rules do not apply to the disclosure of non-identifying health information. A custodian may disclose non-identifying health information for any purpose **(section 32(1))**. However, if non-identifying health information is disclosed to a person who is not a custodian, the custodian must inform the person that the Commissioner must be notified if the person intends to use the information for data matching. **"Data matching"** is defined in **section 1(1)(g)**. The Commissioner must be notified of this intention prior to the data matching being performed **(section 32(2))**.

See section 5.4 of Chapter 5 of this Publication for more discussion on data matching.

A custodian may disclose individually identifying health information to the individual who is the subject of the information, to a representative of the individual (as defined in **section 104(1)(c) to (l)** or, subject to the exceptions set out in **sections 35 to 40, 46, 47 and 53,** to other persons with the individual's consent. Individually identifying diagnostic, treatment and care information may be disclosed by a custodian without the consent of the individual that it is about for certain limited and specific purposes stated in the *Act*, including disclosure to another custodian for any of the purposes listed in **section 27(1) and (2)**.

Individually identifying registration information and health services provider information may also be disclosed without the consent of the individual it is about for certain limited and specific purposes stated in the *Act*.

There are also specific rules in the *Act* related to the disclosure of individually identifying diagnostic, treatment and care information and individually identifying registration information for research purposes

8.2.1 DUTY TO DISCLOSE HEALTH INFORMATION WITH THE HIGHEST DEGREE OF ANONYMITY POSSIBLE

Custodians disclosing health information must consider the level of anonymity that is needed for the intended purpose. They must first consider whether the disclosure of aggregate health information will be adequate for the intended purpose and if so, must only disclose aggregate health information **(section 57(2))**.

"Aggregate health information" is defined in **section 57(1)** to mean non-identifying health information about groups of individuals.

If the custodian believes that disclosing aggregate health information will not be adequate for the custodian's intended purpose, the custodian must then consider whether disclosure of other non-identifying health information is adequate for the intended purpose, and if so, the custodian must disclose the other non-identifying health information **(section 57(3))**.

"Non-identifying health information" is defined in **section 1(1)(r)** to mean that the identity of the individual who is the subject of the information cannot be readily ascertained from the information.

Under **section 57(4)**, if the custodian believes that disclosing aggregate or other non-identifying health information will not be adequate for the custodian's intended purpose, the custodian may disclose individually identifying health information if the disclosure is:

- authorized by the *Health Information Act;* and
- carried out in accordance with the *Health Information Act.*

Under **section 65**, a custodian may strip, encode or otherwise transform individually identifying health information to create non-identifying health information.
(See section 5.3.1 of Chapter 5 of this Publication for a discussion of transforming health information).

"Individually identifying health information" is defined in **section 1(1)(q)** to mean that the identity of the individual who is the subject of the information can be readily ascertained from the information.

"Readily ascertained" in the context of **section 57,** means that the identity of an individual (e.g. the individual's name or other identifiers or distinguishing characteristics associated with an individual) can be determined or deduced without having to apply a sophisticated technical method or process, or without having the particular technical expertise to do so.

An individual's identity can be said to be "readily ascertained" if his or her identity can be determined by:

- combining available information within the same or in several different records;
- comparing information representing distinguishing characteristics with other information sources having both the distinguishing characteristics and the names or other identifiers of individuals; and
- if only readily available or conventional computer hardware, software and technical expertise is used.

Section 57 does not apply where the disclosure of health information is for the purpose of providing a health service (as defined in **section 1(1)(m)**), or for determining the eligibility of an individual to receive a health service.

See section 5.2.1 of Chapter 5 of this Publication for a more detailed discussion of this duty.

8.2.2 DUTY TO DISCLOSE HEALTH INFORMATION IN A LIMITED MANNER

In addition to complying with **section 57**, custodians must only disclose the amount of health information that is essential to enable the custodian or the recipient of the information, as the case may be, to carry out the intended purpose **(section 58(1))**.

Not all of the health information created and maintained by a custodian is relevant or necessary to carry out a certain purpose or address a request for information. Even if a custodian is required by the *Health Information Act* or another act to disclose health information, it should be done by disclosing the least amount possible to achieve the intended purpose.

For example, a physician would not release a patient's complete file without knowing who the information is being disclosed to, why it is needed and whether the same purpose could be achieved by releasing less information. Even if the *Act* requires the disclosure of individually identifying health information, the personal health number, date of service and a code indicating the type of service might be sufficient.

Expressed Wishes of Individual

In deciding how much health information to disclose, a custodian must consider any expressed wishes of the individual who is the subject of the information, together with any other factors the custodian considers relevant **(section 58(2))**. If a patient asks a physician not to tell family members about his or her medical condition, the physician would have to consider whether it was necessary to override those expressed wishes.

An example of a relevant factor that could override the expressed wishes of an individual might be the need for a psychiatrist to have a full and complete medical and psychiatric history of an individual who is not competent, in order to treat a current mental illness even if the individual does not wish to divulge any of this information.

See section 5.2.2 of Chapter 5 of this Publication for a more detailed discussion of this duty.

8.2.3 APPLYING THE 'NEED TO KNOW' PRINCIPLE TO THE DISCLOSURE OF HEALTH INFORMATION BY AFFILIATES

Just as the *Health Information Act* limits the authority of affiliates to collect and use health information, it also limits the authority of affiliates to disclose health information. Under **section 43,** an affiliate of a custodian must not disclose health information in any manner that is not in accordance with the affiliate's duties to the custodian.

This means that unless the disclosure of the information is necessary for the affiliate to carry out one of its/his/her designated responsibilities, the information should not be disclosed by that affiliate. This also implies that custodians must identify the roles and responsibilities of their affiliates and ensure that affiliates are informed about their duties and responsibilities. These roles and responsibilities will limit the amount and the level of anonymity of health information that an affiliate will need to disclose.

In the context of a hospital setting, those affiliates who are directly involved with assessment, diagnosis, treatment and care of an individual may need to disclose individually identifying diagnostic, treatment and care information about the individual, e.g. to other custodians.

Pharmacy and dietary personnel might need to disclose information about the medications or dietary restrictions of a patient moving from an acute care hospital to a long-term care facility but would not need to disclose other individually identifying information that was not relevant to their duties and responsibilities but which may have come to their attention as members of the hospital treatment or care team.

In a multi-unit facility, staff in one unit would usually not have to disclose individually identifying information to the staff of another unit unless the staff in the other unit were covering off due to a staff shortage or an emergency situation.

8.2.4 LIMITS ON THE DISCLOSURE OF NON-RECORDED HEALTH INFORMATION

While the *Act* applies primarily to health information that is written or otherwise recorded and stored, it also places a duty on custodians and their affiliates to protect the confidentiality of information that is not recorded. Early knowledge of various types of health information by health professionals is often oral information (i.e. not written or recorded in any manner at the time the information is collected).

"Confidentiality" implies a trust relationship between the person supplying information and the individual or organization collecting it. The relationship is built on the assurance that the information will only be used by or disclosed to authorized persons or to others with the individual's permission.

Section 44 states that a custodian that collects diagnostic, treatment and care information **(as defined in section 1(1)(i))**, health services provider information **(as defined in section 1(1)(o))**, or registration information **(as defined in section 1(1)(u))** that is not written, recorded or stored in some manner in a record may disclose the information only for the purpose for which the information was provided to the custodian.

This means that if a custodian or its affiliates collect or become aware of the above types of information related to an individual but the information is not recorded, it can still only be disclosed for the purpose for which it was collected.

For example, if the information that is being disclosed was provided to the custodian for the purpose of disclosure to a home care nurse, and was not written or recorded, this information may only be disclosed to the to the home care nurse.

8.2.5 DUTY TO ENSURE AUTHORIZED RECIPIENT

Section 45 states that a custodian that discloses health information must make a reasonable effort to ensure that the person to whom the disclosure is made is the person intended and authorized to receive the information.

"Making a reasonable effort" in the context of this section would mean verifying and authenticating the identity of any individual to whom health information is going to be disclosed prior to the disclosure occurring. This ensures that individuals who request that health information be disclosed to them are who they say they are.

The most common way of authenticating identity in the electronic world is through the use of passwords. However, it could also include requiring proof of identity using tokens, biometrics, challenge/response scenarios, digital signatures and certification authorities in more sophisticated information systems or where the information being disclosed is particularly sensitive. **See section 5.2.4 in Chapter 5 of this Publication for the criteria for authentication passwords.**

In the non-electronic world, custodians should require proof of an individual's identity, particularly before disclosing individually identifying health information to him or her. That proof could be in the form of photo identification, a birth certificate, etc.

8.3 DISCLOSURE OF INDIVIDUALLY IDENTIFYING HEALTH INFORMATION TO THE SUBJECT OF THE INFORMATION

A custodian may disclose individually identifying health information to the individual who is the subject of the information or to a person referred to in **section 104(1)(c) to (i)** who is acting on behalf of that individual **(section 33)**.

If disclosure is made to the individual who is the subject of the information or to the individual's representative, custodians should ensure that they are disclosing the information to persons who are authorized and intended to receive the information **(section 45). See section 8.2.5 above.**

Individually identifying health information may be disclosed to a person representing or acting on behalf of the individual who is the subject of the information. The persons who may act in a representative capacity include:

- the guardian of a minor;
- the personal representative of a deceased individual if the deceased was 18 years of age or older immediately before death and if the disclosure relates to the administration of the individual's estate;
- a guardian or trustee appointed under the *Dependent Adults Act,* if the disclosure relates to the powers and duties of the guardian or trustee;
- an agent designated under a personal directive under the *Personal Directives Act,* if the directive authorizes the disclosure;
- an attorney under a power of attorney if the disclosure relates to the powers and duties conferred;
- the nearest relative of a formal patient under the *Mental Health Act* if the disclosure is necessary to carry out the obligations of the nearest relative under that *Act;* or
- any person with written authorization from the individual.

8.4 DISCLOSURE OF INDIVIDUALLY IDENTIFYING HEALTH INFORMATION WITH CONSENT

The disclosure provisions in the *Act* begin with the concept that an individual should consent to the disclosure of his or her own individually identifying health information. Subject to the exceptions to this contained in **sections 35 to 40, 46, 47 and 53**, a custodian may disclose individually identifying health information to a person other than the individual who is the subject of the information, or the individual's representative **(section 104(1))** if the individual has consented to the disclosure **(section 34)**.

8.4.1 REQUIREMENTS FOR CONSENT

For the purposes of **section 34(1)**, consent must include:

- an authorization for the custodian to disclose the health information specified in the consent;
- the purpose for which the health information may be disclosed;
- the identity of the person to whom the health information may be disclosed;
- an acknowledgement that the consenting individual has been made aware of the reasons why the health information is needed and the risks and benefits to the individual of consenting or refusing to consent to the disclosure;
- the date the consent is effective and the date on which the consent expires; and
- a statement that the consent may be revoked at any time by the individual providing it.

A consent or revocation of consent must be provided in writing or electronically **(34(2))**. Under **section 5(1)** of the Health Information Regulation, an **"electronic consent"** means one that is provided electronically. An **"electronic consent or revocation of consent" (see section 8.5.2 following)** means the granting or revoking of an authority that is provided electronically.

A consent provided electronically by an individual **("electronic consent")** is **not** the same thing as a consent by an individual to the disclosure of his or her individually identifying diagnostic, treatment and care information by electronic means in **section 59(1)**. A separate consent is needed in order for a custodian to disclose this type of health information by electronic means. **See section 5.2.3 of Chapter 5 of this Publication for more information on consent (electronic or written) for the purposes of section 59.**

A disclosure of health information with consent must be carried out in accordance with the terms of the consent **(34(3))**.

A consent that is provided in writing must be signed by the person providing it **(34(5))**. A consent that is provided electronically is valid only if it complies with the requirements set out in the regulations **(34(6))**. Under **section 5(2)** of the Health Information Regulation, an electronic consent or revocation of consent is valid only if the level of authentication is sufficient to identify the individual who is granting or revoking the consent.

Except for the provisions of the *Act* which authorize the disclosure of individually identifying diagnostic, treatment and care information without consent **(section 35)**, and other individually identifying health information, registration information and health services provider information **(sections 36 to 40)**, the absence of consent is interpreted as the absence of authority. True consent is informed and voluntary. Individuals cannot be penalized for refusing to consent to certain disclosures through the denial of the provision of health services, particularly if that was the purpose for which the information was originally collected.

Provision by an individual of his or her personal health number is not the same as consent for disclosure of individually identifying health information.

8.4.2 DISCLOSURE OF DIAGNOSTIC, TREATMENT AND CARE INFORMATION FOR ORGAN DONATIONS AND TRANSPLANTS WITH ORAL CONSENT

Under **section 4(1)** of the *Human Tissue Gift Act,* an individual may consent in writing or orally in the presence of at least 2 witnesses during his last illness that his body or (a) part(s) specified in the consent be used after his/her death for therapeutic purposes, medical education or scientific research.

Under **section 5(1)** of the *Human Tissue Gift Act,* when an individual of any age who has not consented to the use of his/her body or parts of it for therapeutic purposes, medical education or scientific research dies, or in the opinion of a physician, is incapable of giving a consent by reason of injury or disease and his death is imminent, the individual's spouse, next of kin or a person lawfully in possession of the body may consent to the use or donation either in writing or orally in the presence of at least 2 witnesses. Consent may also be given by the spouse, next of kin or other person in lawful possession of the body, by telegraphic, recorded telephonic or other recorded message.

Section 5(2) of the *Human Tissue Gift Act* states that no person shall give a consent under **subsection (1)** if there is reason to believe that the person who dies or whose death is imminent would have objected to it.

In an organ donation/transplant situation as above, the disclosure of the individual's diagnostic, treatment and care information would also be necessary to determine the suitability of the tissue donor.

***BEST PRACTICE:** Since the Act does not expressly provide for oral consent, before disclosing individually identifying health information of the deceased or of an individual whose death is imminent for the purposes of donation of organs or other tissue, first check to see if the individual has previously provided written consent to the donation of tissue in the event of his death. The written consent to donate an individual's tissue could be taken as implied consent to the disclosure of health information necessary to carry out the donation, including disclosure to determine the suitability of the donor or the tissue.*

*If there is no written consent, obtain oral consent from the spouse, next of kin or other substitute decision-maker referred to in **section 104 (1)(c)** to **(i)** of the Health Information Act in the presence of at least 2 witnesses and then document the oral consent. Ask the substitute decision-maker whether the deceased or dying individual had expressed any objections previously to the donation of tissue and, by implication, to the disclosure of health information necessary to carry out the tissue donation.*

*If oral consent cannot be obtained, determine if the disclosure of the individual's health information related to the donation, without the individual's consent, would be permitted under **section 35(1)** of the Health Information Act:*

- *to another custodian for the provision of health services or for any other authorized purpose under **section 27** of the Health Information Act **(35(1)(a)**;*

- *to any person if the custodian believed, on reasonable grounds, that the disclosure would avert or minimize an imminent danger to the health of any person (i.e. an organ transplant could save another's life but individually identifying diagnostic, treatment and care information of the potential donor needs to be disclosed to determine the suitability of the donor) (35(1)(m));or*
- *if the individual lacks the mental capacity to provide the consent and the custodian feels that disclosure would be in the best interests of the individual (35(1)(n));*

If oral consent cannot be obtained, and if none of the exceptions in ***section 35(1)*** *apply, or there is reason to believe that the person who died or whose death is imminent would have objected to the donation and disclosure of related health information, don't disclose the individual's individually identifying health information.*

8.4.3 REQUIREMENTS FOR REVOCATION OF CONSENT

A **"revocation of consent"** means taking away the authority for the consent.

A revocation of consent must be provided in writing or electronically **(section 34(4))**. If the revocation is provided in writing, it must be signed by the person providing it **(section 34(5))**. A revocation of consent that is provided electronically is valid only if it complies with the requirements set out in **section 5(2)** of the Health Information Regulation **(section 34(6))**.

8.5 DISCLOSURE OF INDIVIDUALLY IDENTIFYING DIAGNOSTIC, TREATMENT AND CARE INFORMATION WITHOUT CONSENT

Section 1(1)(i) defines diagnostic, treatment and care information. In certain, limited situations, custodians may disclose individually identifying diagnostic, treatment and care information without an individual's consent. However, as "gatekeepers" of health information, they must still disclose the least amount of information **(section 58)** with the highest degree of anonymity **(section 57(2))**. They must also consider any expressed wishes of the individual who is the subject of the information, together with any other relevant factors **(section 58(2))**.

Note that under **sections 35(1)(c), (d) and (j)**, custodians may disclose individually identifying diagnostic, treatment and care information for certain purposes but must consider whether the disclosure would be contrary to the express request of the individual. Custodians should have policies in place that will accommodate these express requests.

The following sections cover the only situations where custodians may disclose individually identifying diagnostic, treatment and care information without the consent of the individual who is the subject of the information.

8.5.1 DISCLOSURE TO ANOTHER CUSTODIAN FOR AUTHORIZED PURPOSES (section 35(1)(a))

Disclosure of individually identifying diagnostic, treatment and care information to another custodian without consent may be done for any of the purposes listed in **section 27(1) or (2)**. These are the same purposes for which a custodian may use individually identifying health information in its custody or under its control.

The purposes include:

- providing health services;
- determining or verifying an individual's eligibility to receive a health service;
- conducting investigations, discipline proceedings, practice reviews or inspections relating to the members of a health profession or health discipline;
- conducting research (with the approval of an ethics committee);
- providing for health services provider education;
- carrying out any purpose authorized by an enactment of Alberta or Canada; and
- for internal management purposes.

Regional health authorities, provincial health boards, the Alberta Cancer Board, the Minister and the department of Alberta Health and Wellness may also disclose this information, within the geographic area in which they have jurisdiction, for the additional purposes of:

- planning and resource allocation;
- health system management;
- public health surveillance; and
- health policy development.

See section 7.3 of Chapter 7 of this Publication for further information and examples of the authorized purposes in section 27.

8.5.2 DISCLOSURE TO A PERSON PROVIDING CONTINUING TREATMENT AND CARE TO THE INDIVIDUAL (section 35(1)(b))

This provision permits the disclosure of individually identifying diagnostic, treatment and care information without the individual's consent to the person providing continuing treatment and care to the individual. For example, if the individual is discharged from the hospital and returning home, disclosure may be necessary so that appropriate home care can be provided.

Under **section 8(4)** of the Health Information Regulation, if a custodian is disclosing health information to a person in a jurisdiction outside Alberta, the custodian must enter into an agreement with the person to whom the health information is being disclosed. This provision does not apply to health information about an individual that is used in a jurisdiction outside Alberta solely for the purpose of providing continuing treatment and care to the individual **(section 8(5)** of the *Health Information Act* Regulation.

8.5.3 DISCLOSURE TO FAMILY MEMBERS OR THOSE IN A CLOSE PERSONAL RELATIONSHIP (section 35(1)(c))

Under this provision, custodians may disclose information about an individual's location, presence, condition, diagnosis, progress and prognosis on that day to family members of the individual or to another person with whom the individual is believed to have a close personal relationship, without the individual's consent. **The disclosure must not be contrary to the express request of the individual.**

"Person in a close personal relationship" could include a common-law spouse, a close friend or other person who can demonstrate that he or she has such a relationship with the individual who is the subject of the information.

This provision would enable a physician to discuss the diagnosis or condition of a patient or their location with a patient's relative or close friend.

BEST PRACTICE: *If an adult patient in hospital has asked his physician not to disclose details of his condition or prognosis to his spouse, then unless there was a requirement in law or a medical emergency, the physician would respect that express request.*

8.5.4 DISCLOSURE TO FAMILY MEMBERS WHERE INDIVIDUAL IS INJURED, ILL OR DECEASED (section 35(1)(d))

Disclosure of individually identifying diagnostic, treatment and care information without the individual's consent under this provision is for the purpose of notifying or contacting family members of an injured, ill or deceased individual or another person with whom the individual is believed to have a close personal relationship or a friend of the individual. **The disclosure must not be contrary to the express request of the individual.**

BEST PRACTICE: *If an injured adult individual has specifically asked that her family not be contacted, the hospital and physician should not try to contact family members since this would be contrary to the patient's express request.*

8.5.5 DISCLOSURE TO AN OFFICIAL OF A PENAL OR OTHER CUSTODIAL INSTITUTION (section 35(1)(e))

This provision enables custodians to disclose diagnostic, treatment and care information that identifies an individual without the individual's consent to an official of a prison or other institution where the individual is being lawfully held or detained but only to allow health services to be provided to the individual.

"Other custodial institution" could include a jail, holding cells, remand centre, juvenile detention facility, or any other facility or institution where an individual is being lawfully detained and cannot leave.

8.5.6 DISCLOSURE TO A PERSON AUTHORIZED TO CONDUCT AN AUDIT (section 35(1)(f))

Disclosure of individually identifying diagnostic, treatment and care information without the individual's consent under this provision may be made to a person authorized to conduct an audit if the person agrees in writing:

- to destroy the information at the earliest opportunity after the audit is concluded; and
- not to disclose the information to any other person except as required to accomplish the audit or to report unlawful or improper conduct by the custodian or a health services provider.

A **"person authorized to conduct an audit"** could be the Auditor General, another person or body established by regulation for audit purposes or an employee or contractor retained under contract to perform audit services. The authority to conduct the audit could be found in a by-law or resolution of the custodian or may be a requirement under a statute, regulation or policy.

"Audit" is defined in **section 1(1)(c)** to mean a financial, clinical or other formal or systematic examination or review of a program, portion of a program or activity.

The conditions that the auditor must agree to before disclosure occurs are meant to ensure that the information is not used for operational or administrative purposes, involving the individuals concerned.

8.5.7 DISCLOSURE TO A QUALITY ASSURANCE COMMITTEE (section 35(1)(g))

This provision enables a custodian to disclose individually identifying diagnostic, treatment and care information without the individual's consent to a committee that has as its primary purpose the carrying out of quality assurance activities within the meaning of **section 9** of the *Alberta Evidence Act.*

A **"quality assurance committee"** means a committee whose purpose is to study, assess and evaluate the provision of health services with a view to continuous improvement of the quality of health care or health services, or the level of skill, knowledge and competence of health service providers. This term only applies to quality assurance committees as defined in **section 9** the *Alberta Evidence Act* and not to other quality assurance committees established within health care bodies to monitor the quality of health services.

Any information disclosed to a quality assurance committee under this provision must not be disclosed to any other person **(section 35(2))** unless it is non-identifying health information disclosed to another committee that has as its primary purpose the carrying out of quality assurance activities within the meaning of **section 9** of the *Alberta Evidence Act* **(section 35(3)** of the *Health Information* Act).

Although several committees may have a role in reviewing the care provided to a specific patient or group of patients, the committee initially receiving the individually identifying information would have a duty to transform the information into non-identifying information unless the subject individuals consented to the disclosure of their identifying information for the purposes of the other committees.

8.5.8 DISCLOSURE FOR THE PURPOSE OF A COURT PROCEEDING (section 35(1)(h))

A custodian may disclose individually identifying diagnostic, treatment and care information without the individual's consent for the purpose of a court proceeding or a proceeding before a quasi-judicial body to which the custodian is a party.

This provision permits the disclosure of this type of health information to the legal representatives of the custodian for use in such proceedings or to members of the quasi-judicial body or court. The disclosure would normally be to, or through the legal representative of the custodian. Such information may be disclosed to the legal representative of other parties to a proceeding in accordance with the court disclosure and discovery rules that apply.

The following criteria, which are not exhaustive, may help in determining whether a body is a **"quasi-judicial body". The wording of these criteria are adapted from criteria in IPC Order 99-025 which dealt with what should be reviewed in determining whether a body is acting in a "judicial or quasi-judicial capacity".**

- Does the body need to conduct a hearing before a decision on the matter can be reached?
- Does the decision or order directly or indirectly affect the rights and obligations of persons?
- Is the adversarial process involved (are there two opposing parties)?
- Does the body have to apply substantive rules to individual cases rather than implementing social and economic policy in a broad sense?

The legislation under which a decision is made will have to be reviewed to see whether the rules of natural justice apply. The nature of the issue to be decided and the importance of the decision for those affected should also be examined.

An example of such a body is the Alberta Health Facilities Review Committee.

8.5.9 DISCLOSURE FOR THE PURPOSE OF COMPLYING WITH A SUBPOENA, WARRANT OR COURT ORDER (Section 35(1)(i))

This provision enables the disclosure of diagnostic, treatment and care information without the individual's consent for the purpose of complying with legal processes that require the production of information. These processes include subpoenas, warrants or orders issued or made by a court, person or body having jurisdiction to compel the production of information or with a rule of court that relates to the production of information (e.g. a provincial justice).

"Subpoena" is a command or summons requiring the attendance of someone as a witness at a court or hearing. It will specify a place and time when testimony on a certain matter will be required and may also order a person to meet the requirements of a court to disclose information.

Time is of the essence with a subpoena since it is usually served with very little notice. Custodians cannot ignore subpoenas since they would risk being cited for contempt of court and, at a minimum, fined.

"Warrant" is a judicial authorization to collect information – in this context, individually identifying diagnostic, treatment and care information.

"Order" is an authoritative command, direction or instruction to produce something – in this context, individually identifying diagnostic, treatment and care information.

Although **section 35(1)(i)** is discretionary, custodians would normally try to comply with court orders, warrants or subpoenas because they are required to do so by law and generally wish to assist in the administration of justice.

Affiliates of custodians should consult with their legal advisor or a knowledgeable colleague when they receive an order, warrant or subpoena in order to determine whether it is sufficient. This means it must refer to information that is actually in the custody or under the control of the custodian; it must have been granted by a justice or person with proper authority and jurisdiction; and the instrument must have been properly served; among other criteria.

BEST PRACTICES: *If the police or any other person has a subpoena, warrant or court order, determine whether it provides authority for the custodian to disclose the information requested. For example, a warrant may not provide authority for a custodian to notify the police that an individual under care, who is wanted on a warrant, is being discharged from the hospital. It may only provide authority for the police to arrest the individual.*

Next, determine whether a person having jurisdiction to compel production of the information, issued the subpoena, warrant or order. For example, a justice of the peace or a judge outside the province may not have jurisdiction to compel the production of information.

If the subpoena, warrant or order provides authority for the custodian to disclose the information requested to the police or other person, release the information on the basis of the subpoena, warrant or order. If the document does not provide authority for the disclosure, consider whether other provisions of the Health Information Act provide the necessary authority to disclose.

The following examples may help illustrate when a custodian may use this discretionary disclosure provision.

BEST PRACTICE SCENARIO #1: *An individual is under care in an acute care facility and is wanted on a warrant. Should the hospital advise the police when the individual is discharged? If there is no warrant but the police intend to charge the individual, should the hospital notify the police of discharge?*

The individual may have consented to disclosure of basic health information requested by the general public, such as whether the individual is a patient or, alternatively has been discharged from the hospital. The police could call and ask whether a named individual has been *discharged since routine discharge times are well known.*

If the individual has not provided consent for this type of routine disclosure, determine whether the subpoena, warrant or order provides authority for the custodian to disclose the information requested by the police or just authority to arrest the individual.

Determine whether the individual has a life threatening injury, the police are investigating an offence involving the injury and whether the individual has expressly refused this disclosure. The custodian may need to request further information from the police to determine whether disclosure can be made under this provision.

Determine whether an imminent danger to health or safety of any person exists. Custodians may need to request more information from the police to determine whether imminent danger exists.

Determine whether other legislation may provide legal authority to disclose the information. For example, if the discharge is against medical advice, provisions under the Mental Health Act governing formal patients who are not on leave or under the Public Health Act governing recalcitrant patients may apply.

***BEST PRACTICE SCENARIO #2:** Police request a list of underage teens admitted to hospital after overdosing on 'ecstasy' at an out-of-control rave. They want this information to interview the teens to try to identify the supplier of the drug. If the police have a warrant that provides authority to release the information requested, the custodian may do so once it is determined that the warrant is sufficient. If there is no warrant or it is insufficient, consider whether other provisions of the Health Information Act might permit the disclosure (e.g. ask the teens or their parents or guardians if they would consent to the disclosure).*

On the other hand, if the police inform the custodian that they have reason to believe that the drug ecstasy is tainted or adulterated with a substance that is dangerous to the health or safety of others to whom the drug is distributed, the custodian should reconsider whether an imminent danger exists and therefore, whether disclosure is enabled under section 38(1)(m). In this case, the disclosure to the police would be intended to avert danger to the health and safety of individuals who may take the drug in the future or individuals who may have taken the drug but have not yet been treated.

For a more detailed discussion on disclosure to the police, refer to the *Disclosure to the Police: Best Practices* document that is available on request from the department.

8.5.10 DISCLOSURE TO POLICE INVESTIGATING AN OFFENCE INVOLVING A LIFE-THREATENING PERSONAL INJURY TO THE INDIVIDUAL (Section 35(1)(j))

This provision permits disclosure of individually identifying diagnostic, treatment and care information without the individual's consent for the purpose of investigating a life-threatening personal injury to the individual, to any police service. Although the language in the *Act* refers to municipal or provincial police services, the policy intent and best practice is for disclosure under this provision to include municipal, provincial (RCMP), aboriginal or regional police services. Note that the disclosure must not be contrary to the express request of the individual.

There is no duty in the *Health Information Act* to report to the police information about victims of violent crimes who may present themselves for treatment. The victim of a crime decides whether they wish to report to or involve the police. There is no legal duty in Canada to assist police in an investigation, and it is not an offence to refuse to assist them. However, it would be an offence to obstruct the police in a lawful investigation of an offence involving a life-threatening injury.

Custodians who are also "public bodies" under the *FOIP Act* should note that **section 35(1)(j)** of the *Health Information Act* is not as broad in its intent as the provision for disclosure to assist in a law enforcement investigation or proceeding under the *FOIP Act*. Under **section 38(1)(o)** of the *FOIP Act*, personal information of individuals may be disclosed to a law enforcement agency in Canada to assist in an investigation undertaken with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result.

The definition of "law enforcement agency" under the *FOIP Act* includes a variety of agencies responsible for enforcing statutes, not just municipal or provincial police services. Further, the definition of "law enforcement" under the *FOIP Act* includes not only police investigations but also administrative and security investigations, which the *Health Information Act* does not refer to.

Section 38(1)(o) of the *FOIP Act* would not apply to the disclosure of health information to the police by custodians who are subject to the *Health Information Act*.

An **"investigation"** refers to a methodical process of examining, inquiring and observing, including the interviewing of witnesses and the victim of a crime.

A **"life-threatening injury"** refers to an injury to an individual that, in the opinion of the custodian, could result in loss of life without medical treatment.

BEST PRACTICE: *If a police officer comes to a health care facility where a patient has presented with a stab wound and asks for information about the patient, first ask the officer to identify him/herself to determine if he or she is a member of a municipal or provincial police service. Next, determine if the individual has consented to the disclosure of information about his general health status (e.g. is he/she critically ill or in stable condition and is he/she a patient admitted to the hospital). If the officer provides the name of the individual, the custodian could disclose the general health information that the patient has consented to disclose.*

Next, determine whether the officer has a warrant providing authority for the custodian to disclose the information requested by the police.

Next, determine whether the police are investigating an offence involving the individual's injury. The officer should be able to provide a case or complaint number or information on the circumstances surrounding the injury so that the custodian can be assured that he or she is investigating a possible offence under a *statute such as the Criminal Code (Canada). The custodian would next determine whether, in the custodian's opinion, the injury is life-threatening. A stab wound to a hand, for example, may not be life-threatening.*

If the injury is determined to be life-threatening, check to see whether the individual has expressly requested that this information not be disclosed. If the individual has requested non-disclosure of the information, determine whether imminent danger exists to the health or safety of any person ***(see section 8.6.13 of this Chapter).***

Depending upon the specific circumstances, other legislation may provide legal authority to disclose the information, but not necessarily to the police. For example, if the victim is a child, the custodian may be required to report this as child abuse pursuant to the Child Welfare Act. If the victim is an adult in care, the custodian may be required to report this as abuse of an adult pursuant to the Protection for Persons in Care Act. If the victim dies unexpectedly, the custodian is then required to report the unexpected death pursuant to the Fatality Inquiries Act. (Note: police are "medical examiner's investigators" under that Act).

For a more detailed discussion on disclosure to the police, refer to the *Disclosure to the Police: Best Practices* document that is available on request from the department.

8.5.11 DISCLOSURE TO ANOTHER CUSTODIAN TO DETECT OR PREVENT FRAUD OR ABUSE OF HEALTH SERVICES (Section 35(1)(k))

This provision authorizes a custodian to disclose individually identifying diagnostic, treatment and care information to another custodian without the individual's consent where the disclosing custodian has a reasonable expectation that disclosure will detect or prevent fraud, limit abuse in the use of health services or prevent the commission of an offence under an enactment of Alberta or Canada.

A **"reasonable expectation"** would be one that would be deemed as fair, proper, just, moderate, rational and suitable under the circumstances and one where there is a clear cause and effect relationship between the disclosure and the expected result with the likelihood of the result being genuine and conceivable.

An **"offence"** could include those under the *Alberta Health Care Insurance Act,* under various statutes of regulated health professionals, or under the *Criminal Code (Canada).*

An example of the use of discretionary disclosure under this provision would be a pharmacist providing information to other pharmacists in a "fan out" about an individual trying to use a suspicious prescription. A pharmacist may also volunteer to coordinate the dissemination of this information to regional pharmacies. The *Criminal Code (Canada)* does not compel custodians to disclose health information (by reporting a possible fraudulent use of a prescription) to the police unless there is a warrant or subpoena that specifically requires disclosure of the specific health information requested.

8.5.12 DISCLOSURE TO AN OFFICER OF THE LEGISLATURE (Section 35(1)(l))

Under this section, individually identifying diagnostic, treatment and care information may be disclosed without the individual's consent to an officer of the Legislature if the information is necessary for the performance of the officer's duties.

Officers of the Legislature are the Auditor General, the Ombudsman, the Chief Electoral Officer, the Ethics Commissioner and the Information and Privacy Commissioner.

Disclosure under this provision is restricted by the requirement that the information is necessary for the performance of the officer's duties. For example, the Ombudsman may be investigating a complaint at the request of an individual involving a decision made by the department that relates to the individual's health information. Individually identifying diagnostic, treatment and care information may also need to be disclosed to the Information and Privacy Commissioner for the purpose of a review of a privacy complaint.

If the reason for the disclosure is not clear from the request, custodians should seek an explanation as to why the individually identifying health information is needed and whether non-identifying information would be sufficient for the purpose.

8.5.13 DISCLOSURE TO AVERT OR MINIMIZE IMMINENT DANGER TO HEALTH OR SAFETY OF ANY PERSON (Section 35(1)(m))

This provision permits the disclosure of individually identifying diagnostic, treatment and care information without the individual's consent to any person, including a municipal or provincial police service if the custodian believes, on reasonable grounds, that the disclosure will avert or minimize an imminent danger to the health or safety of any person.

Three criteria must be satisfied for **"imminent danger"** to exist:

- clarity – the intended victim or group of victims must be ascertainable or sufficiently identifiable;
- danger – the danger to the victim must be serious bodily harm or death; and
- imminence – the risk must be serious and a sense of urgency must be created by the threat of danger. The risk could be a future risk but must be serious enough that a reasonable person would be convinced that the harm would be carried out.

These three criteria must be considered in the context of each situation and in view of the surrounding circumstances. There must be a clear and imminent threat of serious bodily harm or death to an identifiable group or person that creates a sense of urgency.

For example, if a victim of a violent crime is being treated in a hospital, and the custodian has determined that the safety of the individual would be in jeopardy (i.e. there is danger of further serious harm occurring), the custodian should seek further information from the police and may need to disclose individually identifying health information to the police in order to avert or minimize the potential of further harm to the individual.

BEST PRACTICE SCENARIO #1: *A physician has a client who is an HIV-positive drug user and learns that the client is sharing needles with other individuals in the community. After considering the reliability of the information and the level of risk to identifiable contacts, the physician should confirm whether others have been exposed or are at risk. He or she should then determine whether the client knows about and is practicing or is willing to practice appropriate safety precautions. Based upon reliable information, the physician may consider reporting the client to the Medical Officer of Health as a recalcitrant patient under the Public Health Act.*

BEST PRACTICE SCENARIO #2: *An individual robbed a bank, carrying a briefcase that he claimed contained an explosive device. He also claimed that he was dying of a terminal illness and had "nothing to lose". Several days after the robbery, police are requesting information from physicians who have treated terminally ill patients fitting the suspect's description.*

It is not clear whether there is imminent danger to the health or safety of any person. The custodian would have to consider whether the individual just made one isolated threat regarding the explosive device during a past incident or whether it is likely that the individual is going on a rampage involving further violence. The custodian may need to seek further information from the police.

The key element is whether the custodian believes, on reasonable grounds, that imminent danger to the health or safety of any person will be minimized or averted by this disclosure.

BEST PRACTICE SCENARIO #3: *A client of a psychiatrist is a pedophile with violent tendencies. The client also has a history of molesting children when using street drugs and is using street drugs again.*

After assessing the reliability of the information and determining that there is a high risk of the client re-offending; and if there are identifiable victims who will be protected by disclosure, the psychiatrist or manager of a treatment facility could release to potential victims the minimum amount of information necessary to warn them of the potential harm. Prior to disclosure, the manager would have to obtain any approvals required within the treatment facility.

The police would not necessarily be notified but depending upon the facts of a situation, involving the police may be part of the strategy.

8.5.14 DISCLOSURE IN THE BEST INTERESTS OF AN INDIVIDUAL WHO LACKS THE MENTAL CAPACITY TO PROVIDE CONSENT (Section 35(1)(n))

Under this provision, a custodian may disclose individually identifying diagnostic, treatment and care information if the individual lacks the mental capacity to consent, does not have a representative or substitute decision – maker under **section 104(1)(c) to 104(1)(i)** and, in the opinion of the custodian, the disclosure is in the best interests of the individual.

Before disclosure of health information occurs under this provision, the custodian is required to form an opinion about two things:

- whether the individual lacks the mental capacity to provide a voluntary and informed consent; and
- whether the disclosure would be in the best interests of the individual.

Both opinions would be based upon the custodian's judgment (if the custodian is a physician or other clinician) or upon the judgment of an affiliate of the custodian who could provide the custodian with an expert opinion about both the mental capacity and best interests of the individual. Whether or not disclosure should occur would also depend upon the circumstances of each individual situation. The custodian should also disclose only the minimum amount of information required to carry out the purpose.

8.5.15 DISCLOSURE TO A DESCENDANT OF A DECEASED INDIVIDUAL, AN AUTHORIZED REPRESENTATIVE OR A PERSON PROVIDING HEALTH SERVICES TO A DESCENDANT (Section 35(1)(o))

This provision allows a custodian to disclose individually identifying diagnostic, treatment and care information to a descendant of a deceased individual, a person referred to in **section 104(1)(c) to 104(1)(i)** who is acting on the behalf of the descendant or a person who is providing health services to the descendant.

However, before disclosure is made, the custodian must first form an opinion that:

- the disclosure is necessary to provide health services to the descendant; and
- the disclosure is restricted sufficiently to protect the privacy of the deceased individual.

Examples of persons referred to in **section 104(1)(c) to 104(1)(i)** would be a parent or guardian of a descendant who is under 18 years of age and does not meet the criterion in **104(1)(b)**, a guardian or trustee under the *Dependent Adults Act,* the nearest relative of a formal patient under the *Mental Health Act,* an individual authorized by a power of attorney, etc.

The disclosure must be necessary to provide health services to the descendant as **"health services"** is defined in **section 1(1)(m)**. The custodian must also restrict the disclosure to protect the privacy of the deceased individual. This would mean limiting the amount of information disclosed to what was absolutely necessary for the provision of health services to the descendant (not the complete medical record of the deceased).

Custodians who are also public bodies under the *FOIP Act* should note that the *Health Information Act* does not have a provision similar to **section 16(2)(i)** of the *FOIP Act* which says that it would not be an unreasonable invasion of a deceased's personal privacy to disclose personal information about an individual who has been dead for 25 years or more.

8.5.16 DISCLOSURE AUTHORIZED OR REQUIRED BY AN ENACTMENT OF ALBERTA OR CANADA (Section 35(1)(p))

This provision permits a custodian to disclose individually identifying diagnostic, treatment and care information without the individual's consent if another enactment of Alberta or Canada authorizes or requires the disclosure.

"Enactment" means an act or regulation or any portion of an act or regulation. The act or regulation must either be an Alberta or federal statute or regulation (not another province's legislation) and must impose an obligation to disclose the health information or, alternatively, authorize or permit the disclosure.

Since disclosures under this provision are discretionary, unless another enactment expressly prevails over the *Health Information Act,* custodians must still exercise their discretion in terms of disclosures of health information that are authorized or required by another enactment.

(See Chapter 12 of this Publication on Consequential Amendments which discusses some of the statutory provisions that prevail over the *Health Information Act*).

Some examples of other legislation that authorizes or requires the disclosure of certain types of individually identifying diagnostic, treatment and care information are:

- ***Criminal Code (Canada)*** provides indirect authority to compel disclosure of information as specified in warrants or subpoenas when the warrant or subpoena specifically requires disclosure of the specific health information requested. Note that this legislation does not compel custodians to disclose health information to the police, for example victims of violent crime with gunshot or stab wounds.

  The ***Criminal Code*** authorizes the release of diagnostic, treatment and care information to a board of review appointed under the ***Criminal Code*** so that the board can review the case of the person to whom the records relate.

- ***Controlled Drugs and Substances Act (repealed the Narcotics Control Act)*** authorizes practitioners such as physicians and pharmacists to possess controlled substances. A justice may issue a search warrant that authorizes a peace officer to search a person or place for a controlled substance and to seize the substance. Under the ***Narcotic Control Regulations (under this Act),*** pharmacists, physicians and hospital employees must furnish information and make all records available to the Minister of Justice, as the Minister requires, permit inspectors to make copies of any records, and report any loss or theft of a narcotic within 10 days to the Minister.

- ***Fatality Inquiries Act*** requires custodians to report unexpected deaths but does not require the disclosure of information about other individuals. This statute would authorize disclosure of health information about an individual who may have died at the scene of an accident to the police if they were acting as medical examiner's investigators under this *Act* with respect to the person who died at the scene.

- ***Protection for Persons in Care Act*** requires custodians to disclose individually identifying health information by reporting on the possible abuse of an adult in care.

- ***Child Welfare Act*** requires a custodian to disclose individually identifying health information by reporting on the possible abuse of a child.

- ***Mental Health Act*** provides for disclosure of individually identifying health information if a formal patient under that *Act* who is not on leave, discharges him/herself against medical advice.

- ***Public Health Act*** provides for the disclosure of individually identifying health information of recalcitrant patients and also requires custodians to notify the Medical Officer of Health regarding certain communicable diseases e.g. AIDS, gonorrhea, botulism, giardiasis, meningitis, just to name a few.

- ***Traffic Safety Act (when proclaimed in force)*** authorizes the Minister responsible for that *Act* to make regulations respecting the notification to the Registrar of Motor Vehicle Services by physicians and optometrists of any condition that a person has that may affect that person's ability to operate a vehicle in a safe manner. The regulations under this section of the *Act* will either authorize or require physicians or optometrists to disclose this kind of information about medical conditions of individuals that may affect their ability to operate a vehicle in a safe manner.

  Currently, under **section 14(2)** of the *Motor Vehicle Administration Act*, physicians are protected from liability if they report medical conditions that might adversely affect a person's ability to operate a motor vehicle. Physicians are not currently required to report this information.

- ***Vital Statistics Act*** requires births and deaths to be reported to the Director of Vital Statistics.

8.5.17 DISCLOSURE TO THE SUCCESSOR OF A CUSTODIAN (Section 35(1)(q))

Under this provision, a custodian may disclose individually identifying diagnostic, treatment and care information without the individual's consent to its successor if:

- the successor is a custodian; and
- it is for the purpose of the custodian transferring its records to the successor as a result of the custodian ceasing to be a custodian.

A **"successor"** would be the person or organization that obtains ownership of or title to a custodian's facility or practice when the custodian ceases to be a custodian. A successor could be an individual, a partnership, corporation or other unincorporated organization or sole proprietorship.

This provision would, for example, enable a physician or other health professional in the publicly funded health system to transfer his or her patient files to another physician who is taking over the practice of that physician.

8.5.18 DISCLOSURE TO A HEALTH PROFESSIONAL BODY (Section 35(4))

This provision authorizes a custodian to disclose individually identifying diagnostic, treatment and care information without the individual's consent to a health professional body for the purpose of an investigation, a discipline proceeding, a practice review or an inspection.

This disclosure may only be done if:

- the custodian has complied with any other enactment authorizing or requiring the custodian to disclose that information for that purpose (e.g. the *Health Professions Act*); and
- the health professional body agrees in writing
  - not to disclose the information to any other person except as authorized by or under the Act governing the health professional body; and
  - to destroy the information at the earliest opportunity if the investigation proceeding, practice review or inspection is abandoned, or at the earliest opportunity after a final decision has been made relating to the investigation, discipline proceeding, practice review or inspection, including any decision made by a body authorized to hear appeals.

A **"health professional body"** is defined in **section 1(1)(l)** as a body that regulates the members of a health profession or health discipline pursuant to an Act. Examples of these bodies are the Alberta Association of Registered Nurses, Alberta College of Optometry, Alberta College of Pharmacists, Alberta Dental Association, College of Physicians and Surgeons of Alberta and College of Physical Therapists of Alberta, among others.

An **"investigation"** refers to a systematic process of examination, inquiry and observation.

A **"discipline proceeding"** refers to a formal process of determining whether a practitioner has displayed a lack of skill or judgment in the practice of his or her profession; has displayed unbecoming and/or unprofessional, disgraceful or dishonourable conduct; or is incapable or unfit to practice his or her profession.

A **"practice review"** refers to an assessment or evaluation of the professional performance or competence of a practitioner.

An **"inspection"** refers to the examination or viewing of the physical premises or of the books, records, papers or other documents of a practitioner as part of an investigation.

The health professional body must agree in writing not to disclose the information except as authorized under the Act governing that health professional body and to destroy the information as soon as possible once the review is complete, a decision is made or the review is abandoned.

8.6 MAINTENANCE OF INFORMATION ON DISCLOSURE OF INDIVIDUALLY IDENTIFYING DIAGNOSTIC, TREATMENT AND CARE INFORMATION (Section 41)

This provision says that when a custodian discloses a record containing individually identifying diagnostic, treatment and care information without consent under **section 35(1) or (4)**, the custodian must make a notation of that disclosure.

The provision only applies to disclosure of a **"record"** as that is defined in **section 1(1)(t)** not to disclosure of health information that is not in a record. For example, a telephone call by a pharmacist to a physician regarding a patient's prescription or a verbal consultation about a patient between a family physician and a specialist would not have to be noted under this provision.

The disclosure notation requirement applies to any disclosure of a record containing individually identifying diagnostic, treatment and care information without the individual's consent. This would include disclosure of individually identifying diagnostic, treatment and care information to another custodian for an authorized purpose under **section 27**.

The notation must include:

- the name of the person to whom the custodian disclosed the information;
- the date and purpose of the disclosure; and
- a description of the information disclosed.

The notation of disclosure information must be retained by the custodian for 10 years following the date of disclosure **(section 41(2))**. This enables an individual who is the subject of the information to ask the custodian for access to and a copy of the information. The provisions in **Part 2** of the *Act* **(Individual's Right to Access Individual's Health Information)** regarding the access request process would apply to this type of request. The request for the disclosure notation information might be a separate request under **section 7(1)** or the records might be included as part of a request for all of an individual's own health information under that section.

Disclosure notations could take a number of forms. They could be in either paper or electronic form but need to be retrievable by individual identifier. The notation could be made on an individual's health record or file in a practitioner's office or on a client's electronic drug record in a pharmacy. If the notation is not made on the individual's file or health record, a "disclosure log" or book could be used to record all disclosures where a notation is required under **section 41.** Alternatively, the notation could take the form of a transmittal memo that is then put into a log or onto the individual's health record or file.

For health authorities and larger clinics, disclosure notations are likely to be made by health records' personnel on the patient's individual chart, file or record and would be accessible to the patient if they made an access request under **Part 2** of the *Act*.

An alphabetical log is preferable to a chronological log so that an individual could access this information about him/herself but care would have to be taken to ensure that disclosure information about other individuals was not disclosed to the applicant.

The maintenance of notations of disclosure is necessary to enable a custodian to comply with its duties under **sections 13 and 14** in response to a request for correction or amendment of health information. Under **section 13,** if a correction or amendment has been made, a notice of the correction or amendment must be provided to any person to whom the health information that is the subject of the applicant's request has been disclosed in the preceding year.

Under **section 14,** if a correction or amendment is refused and the individual submits a statement of disagreement, the custodian must provide the statement of disagreement to any person to whom the custodian has disclosed the record in the year preceding the applicant's request.

8.7 NOTIFICATION OF RECIPIENT OF PURPOSE AND AUTHORITY FOR DISCLOSURE OF DIAGNOSTIC, TREATMENT AND CARE INFORMATION (Section 42)

A custodian that discloses individually identifying diagnostic, treatment and care information must inform the recipient in writing of the purpose of the disclosure and the authority under which the disclosure is made **(section 42(1)). Section 42(2)** says that this provision does not apply where the disclosure is:

- to another custodian under **section 35(1)(a)** (for authorized purposes under **section 27** – e.g. providing health services or managing the health system);
- to the Minister or the Department under **section 46**; or
- to certain other custodians under **section 47**.

Recipients of health information must not:

- use the information for direct commercial marketing or fundraising purposes without consent **(section 107(2)(f))**;
- take steps to re-identify an individual from non-identifying health information through data matching without first notifying the Information and Privacy Commissioner **(section 32(2))**; or
- require an individual to provide their personal health number unless they have that authority under **section 21** of the Health Information Regulation and cannot use the number for any additional purpose.

For the various forms of Notices to Recipients, see Appendix 1 of this Publication.

8.8 DISCLOSURE OF INDIVIDUALLY IDENTIFYING DIAGNOSTIC, TREATMENT AND CARE INFORMATION BY ELECTRONIC MEANS (Section 59(1))

A custodian that intends to disclose individually identifying diagnostic, treatment and care information about an individual by electronic means must obtain the individual's consent (either written or electronic consent) to the means of disclosure or ensure that the individual's consent has been previously obtained.

This is a positive duty that custodians must comply with. However, if the disclosure is for the purpose of obtaining or processing payment for health services, the information may be disclosed by electronic means without the individual's consent **(section 59(7)**.

See section 5.2.3 of Chapter 5 of this Publication for a more detailed discussion of "electronic means" and the process for obtaining consent for this form of disclosure.

8.9 DISCLOSURE OF REGISTRATION INFORMATION WITHOUT CONSENT (Section 36)

Under this provision, a custodian may disclose individually identifying registration information without the individual's consent for the following purposes:

- for any purposes for which diagnostic, treatment and care information may be disclosed under **section 35(1) or (4) (see section 8.5 of this Chapter for the types of recipients)**;
- to any person for the purpose of collecting or processing a fine or debt owing by the individual to the Government of Alberta or to a custodian; or
- to a person who is not a custodian if the disclosure is in accordance with the requirements set out in the regulations.

"Registration information" is defined in **section 1(1)(u)** as information relating to an individual that falls within the following general categories and is more specifically described in the Health Information Regulation:

- demographic information (such as name, photograph, gender, personal health number, date of birth, etc.);
- location, residency and telecommunications information (such as home mailing address, electronic address, citizenship and immigration status, date of entry into Canada and into Alberta, etc.);
- health service eligibility information, such as whether the individual is registered as a registrant or dependant under the *Health Insurance Premiums Act,* whether the individual is exempt from the requirement to register or pay premiums under that *Act,* etc.); and
- billing information (such as information about amounts owed by the individual to the custodian, method of payment, the individual's account number, etc.).

but does not include information that is not written, photographed, recorded or stored in some manner in a record.

For the purposes of **section 1(1)(u), section 3** of the Health Information Regulation lists the information relating to an individual that is included in the term "registration information".

An individual's account number has been included in registration information to ensure that the collection, use and disclosure of these numbers can be regulated. Custodians have a duty to protect account numbers. Custodians may be fined if account numbers are inappropriately disclosed.

BEST PRACTICE:* *Custodians should not disclose individuals' account numbers except with consent.

Under **section 36(b), "collecting a debt"** can include billing for payment since this is part of collecting and processing the debt. The debt exists when the custodian has finally stated what their bill is and has recorded this in their own records or books.

For the purposes of **section 36(c)**, a custodian may disclose to an ambulance attendant or operator under the *Ambulance Services Act* individually identifying registration information about an individual without the consent of the individual (**section 7** of the Health Information Regulation).

Custodians need to be very cautious in disclosing registration information even if it is just a name and address. If the disclosure of registration information could reasonably be expected to result in harm to the individual's mental or physical health or safety, the custodian should first obtain the individual's consent or transform the information so that it becomes non-identifying information.

8.10 DISCLOSURE OF HEALTH SERVICES PROVIDER INFORMATION WITHOUT CONSENT (Section 37)

Under **section 37(1)**, a custodian may disclose individually identifying health services provider information without the individual's consent for the following purposes:

- to a health professional body that requests the information for the purpose of an investigation, a discipline proceeding, a practice review or an inspection relating to the health services provider; or
- if the disclosure is authorized or required by an enactment of Alberta or Canada.

"Health services provider" is defined in **section 1(1)(n)** as an individual who provides health services.

"Health services provider information" is defined in **section 1(1)(o)**.

See section 8.5.18 of this Chapter for the definitions of "health professional body", "investigation", "discipline proceeding", "practice review" and "inspection".

The disclosure may be authorized or required by another enactment of Alberta or Canada. Rules regarding the disclosure of health services provider information for each health profession are generally found in the health professional statute, such as the *Medical Profession Act, Nursing Profession Act, etc.* (or in the *Health Professions Act* once that is proclaimed in force and becomes applicable to each health profession). Health professional bodies maintain public registers of their members that contain information as required by their governing statute. In some cases, these registers are available on-line.

Under **section 37(2)**, custodians may disclose the health services provider information described in **section 1(1)(o)(i) to (iii), (vii), (xiv), (xv), (xviii) and (xix)**, other than home address, telephone number and licence number, to any person for any purpose without the consent of the individual unless the disclosure:

- would reveal other information about the health services provider; or

- could reasonably be expected to result in harm to the health services provider's mental or physical health or safety, or undue financial harm to the health services provider.

This provision enables custodians to disclose basic "business card" information about a health services provider (e.g. name, business and electronic address, business fax and telephone numbers, profession, job classification, employer, etc.) to any person for any purpose unless the disclosure could result in physical or emotional harm to the individual or cause undue financial harm. Physical harm to an individual provider could result, for example, from the disclosure of a home address of a physician providing abortion services to patients.

8.11 DISCLOSURE OF INDIVIDUALLY IDENTIFYING HEALTH INFORMATION WITHOUT CONSENT TO AN ARCHIVES (Section 38)

This provision permits a custodian to disclose individually identifying health information without the individual's consent to the Provincial Archives of Alberta or to any other archives that is subject to the *Health Information Act* or to the *FOIP Act* for the purposes of permanent preservation and historical research if, in the opinion of the custodian, the information has enduring value.

An **"archives"** could be the custodian's own archives, in which case the health records would remain in the custody or under the control of the custodian. It could be the archives of another custodian or public body under the *FOIP Act* in which case, custody and control of the records would normally be transferred to the archives. It could be an archival facility that operates as an affiliate of a custodian through a contract or agency relationship. In this situation, custody may be transferred but control must be retained by the custodian.

This provision does not permit disclosure to a private archives such as one operated by a private museum or historical society.

Before disclosure takes place under this provision, the custodian must first determine whether the information has enduring value.

8.12 DISCLOSURE BY MINISTER OR DEPARTMENT (Section 39)

Under **section 39(1)**, the Minister or department may disclose individually identifying diagnostic, treatment and care information without the consent of the individual who is the subject of the information to another Minister of the Government of Alberta for the purpose of developing public policy.

Examples of this purpose would be the disclosure of information on specific types of cases so that services to those individuals can be coordinated across various government departments in Alberta or the disclosure of information to develop programs or services for specific target populations where they are going to be delivered by various government departments – e.g. programs for children, seniors, etc.

Section 39(2) enables the Minister or department to enter into an agreement with another Minister of the Government of Alberta or a Minister of the Government of

Canada or of any other province, or a person or entity in accordance with regulations made under the *Alberta Health Care Insurance Act,* respecting the disclosure of individually identifying registration information without the consent of the individual who is the subject of the information.

Agreements under this provision may be needed to establish the mechanisms and accountability structures for federal-provincial or inter-provincial funding of health programs or services.

8.13 DISCLOSURE TO MINISTER (Section 40)

Under this section, a custodian other than the Minister may disclose individually identifying health information to the Minister without the consent of the individual who is the subject of the information if, in the opinion of the custodian, the disclosure is necessary or desirable to enable the Minister to carry out the duties of the Minister.

The disclosure of individually identifying information to the Minister under this section is discretionary. In forming an opinion about whether the information is necessary or desirable to enable the Minister to carry out the duties of the Minister, the custodian must first apply the principles of disclosing the least amount of information **(section 58(1)),** at the highest level of anonymity **(section 57)),** and must consider as an important factor any expressed wishes of the individual who is the subject of the information **(section 58(2))**. The custodian should also ensure that the reason for disclosing the information is to enable the Minister to carry out his ministerial responsibilities, not for other purposes unrelated to those responsibilities or duties.

8.14 DISCLOSURE FOR HEALTH SYSTEM PURPOSES

Sections 46 and 47 permit the disclosure of individually identifying health information to the Minister or department or to regional health authorities, the Alberta Cancer Board to the Alberta Mental Health Board for any of the authorized purposes listed in **section 27(2)**.

The authorized purposes in **section 27(2)** which can only be carried out within the geographic area in which the custodian has jurisdiction to promote the objectives for which the custodian is responsible are:

- planning and resource allocation;
- health system management;
- public health surveillance; and
- health policy development.

Refer to section 7.4.2 in Chapter 7 of this Publication for more information and examples of these authorized purposes.

8.14.1 DISCLOSURE TO MINISTER AND DEPARTMENT (Section 46)

Under **section 46(1),** the Minister or department may request another custodian to disclose individually identifying health information for any of the **section 27(2)** purposes if:

- the Minister or the Department is authorized by an enactment of Alberta or

Canada to obtain the information from the other custodian **(section 46(1)(a))**; or

- the information relates to a health service provided by the other custodian that is:
  - fully or partially paid for by the department, or
  - provided using financial, physical or human resources provided, administered or paid for by the department **(section 46(1)(b))**.

See section 1(1)(m) of the *Act* for a definition of **"health service"**.

"Fully paid" refers to health services that are funded completely by the department.

"Partially paid" refers to health services that are partially funded by the department (e.g. a portion of chiropractic services) with the rest of the services being paid for privately.

In addition to health services that are fully or partially paid for by the department, if the health service is provided through the use of financial (money), physical (building, equipment) or human (employees or other affiliates) resources that are provided, administered or paid for by the department, disclosure of the health information would fall within **section 46(1)**.

If the requirements of **section 46(1)(a) or (b)** are met, **subject to section 46(5),** the custodian **must** disclose the information requested **(section 46(2)**.

The Minister or the department may disclose the information received to a regional health authority, the Alberta Cancer Board or the Alberta Mental Health Board for any of the **section 27(2)** purposes **(section 46(3))**. The information may be disclosed without the consent of the individual who is the subject of the information **(section 46(4))**.

However, before the Minister or department discloses the individually identifying information to them under **section 46(3)**, it must:

- prepare a Privacy Impact Assessment (PIA) describing how disclosure of the health information may affect the privacy of the individual who is the subject of the information, and submit it to the Commissioner for review and comment, and
- consider the comments of the Commissioner, if any, made in response to the PIA **(section 46(5))**.

In addition to following the procedure outlined in the section, the Minister or department would have to consider collecting the least amount of information at the highest level of anonymity, along with having to demonstrate a need to know the information that is being requested. In most cases, non-identifying health information will be sufficient. For example, aggregate information would likely be sufficient for health system management purposes.

8.14.2 DISCLOSURE TO RHA'S, ALBERTA MENTAL HEALTH BOARD, ALBERTA CANCER BOARD (Section 47)

Under **section 47(1)**, certain other custodians (e.g. the Alberta Cancer Board) may request a custodian (e.g. a physician, approved hospital, the department, etc.) to disclose to the requesting custodian individually identifying health information for any of the **section 27(2)** purposes if:

- the requesting custodian is authorized by an enactment of Alberta or Canada to obtain the information from the other custodian **(section 47(1)(a)**; or
- the information relates to a health service provided by the other custodian that is:
  - fully or partially paid for by the requesting custodian; or
  - provided using financial, physical or human resources provided, administered or paid for by the requesting custodian. **(section 47(1)(b))**

See the discussion under section 8.14.1 of this Chapter regarding a "health service" and "fully or partially paid for".

Unless the disclosure is authorized by an enactment of Alberta or Canada, under **section 46(2)**, the custodian receiving the request may refuse to disclose the information if the disclosure could reasonably be expected:

- to result in immediate and grave harm to the mental or physical health or safety of the individual who is the subject of the information;
- to threaten the mental or physical health or safety of another individual; or
- to pose a threat to public safety.

See section 3.3.1 (Discretionary Exceptions) in Chapter 3 of this Publication for an explanation and examples of immediate and grave harm, threatening mental or physical health or safety and threatening public safety.

If a custodian refuses to disclose information because of the factors in **section 47(2)**, the custodian must provide the requesting custodian with non-identifying health information in the form requested by that custodian, and the requesting custodian may ask for a review by the Commissioner of the refusal to disclose **(section 47(3))**.

If the custodian refusing to disclose is a member of a health professional body, the Commissioner must inform that body of the review and provide an opportunity for that body to make comments relating to the review **(section 47(4))**.

In addition to following the procedure outlined in the section, a custodian such as a health authority would have to consider collecting the least amount of information at the highest level of anonymity, along with having to demonstrate a need to know the information that is being requested. There would be very limited situations where a health authority would be requesting identifiable health information from other custodians (e.g. physicians). In most cases, non-identifying health information will be sufficient. For example, aggregate information would likely be sufficient for health system management purposes.

Once the requesting custodian receives health information under this section, it may disclose the information to regional health authorities, the Alberta Mental Health Board or the Alberta Cancer Board, the Minister or department for any of the **section 27(2)** purposes **(section 47(5))**. Individually identifying health information may be disclosed under **section 47** without the consent of the individual who is the subject of the information.

8.15 DISCLOSURE FOR RESEARCH PURPOSES

Division 3 of Part 5 of the *Act* sets out the rules for custodians and researchers regarding the disclosure of health information for research purposes.

"Research" is defined in **section 1(1)(v)** to mean academic, applied or scientific health-related research that necessitates the use of individually identifying diagnostic, treatment and care information or individually identifying registration information, or both.

"Health information" for the purposes of **Division 3 of Part 5** means individually identifying diagnostic, treatment and care information or individually identifying registration information, or both.

8.15.1 SUBMISSION OF A RESEARCH PROPOSAL TO AN ETHICS COMMITTEE

Under **section 49,** a person who intends to conduct research (as defined in **section 1(1)(v)**) may submit a proposal to an ethics committee for review by that committee. Although the wording in this section appears to be permissive, **sections 27(1)(d) and 52** require research proposals to be submitted for review.

An **"ethics committee"** as defined in **section 1(1)(j)** means a committee designated by the regulations as an ethics committee.

The ethics committees referred to in the *Act* are commonly referred to as research ethics boards in the research community. This definition also does not include clinical or bio-clinical ethics review committees. Some ethics committees work conjointly with other bodies, such as health authorities. The University committees, for example, have this broader mandate.

The Designation Regulation lists the following committees and boards as ethics committees for the purposes of **Part 5, Division 3** of the *Act*:

- Alberta Cancer Board – Research Ethics Committee;
- College of Physicians and Surgeons of Alberta – Research Ethics Review Committee;
- Alberta Heritage Foundation for Medical Research – Community Health Ethics Research Review Committee;
- University of Alberta – Health Research Ethics Board;
- University of Calgary – Conjoint Health Research Ethics Board;
- University of Lethbridge – Human Subject Research Committee.

In order to be eligible for and to maintain designation under the *Health Information Act,* an ethics committee must meet the following criteria:

- consist of at least 5 members, including both men and women:
  - at least 2 of whom have broad expertise in research methods;
  - at least one of whom is knowledgeable in research ethics;
  - at least one of whom is knowledgeable in the area of protection of individual privacy;
  - at least one of whom represents the community served by the ethics committee;
- operate under the sponsorship of a research institution, professional body,

regional health authority or other publicly funded body;

- undertake at least 12 to 24 ethics reviews per year as the primary ethics review board;
- arrange appointments to the committee to balance the need to maintain continuity with the need to ensure diversity of opinion and the opportunity to spread knowledge and experience gained from membership throughout the hosting organization and community.

A board or committee wishing to be designated under the Designation Regulation may apply to the Minister of Alberta Health and Wellness by providing the following information about the proposed ethics committee:

- its terms of reference;
- its authorities and responsibilities;
- its requirements for submission of research proposals;
- demonstration of compliance with the standards set by the *Tri-Council Policy Statement on Ethical Conduct for Research Involving Humans (September 17, 1998* or later versions as they are implemented);
- its frequency/structure of meetings;
- its membership and membership selection/replacement process (for committees who would normally not disclose the names of members, providing the Minister with a listing of the areas of expertise and gender of the members may be sufficient); and/or
- a description of its relationships with any other ethics committees within the institution/organization.

The Tri-Council is a consortium of three federal research funding Councils – the Canadian Institutes of Health Research (CIHR), formerly Medical Research Council (MRC)), the Natural Sciences and Engineering Research Council (NSERC) and the Social Sciences and the Humanities Research Council (SSHRC). The Tri-Council policy statement replaced the previous MRC and SSHRC guidelines with an updated and more comprehensive document covering all research with human subjects supported by the three Research Councils.

The Minister retains the authority to remove an ethics committee's designation under the Designation Regulation if it fails to maintain the required criteria for designation.

8.15.2 ROLE OF ETHICS COMMITTEES

Under **section 50(1)**, an ethics committee reviews proposals to conduct research. The review must:

- consider whether the researcher should be required to obtain consents for the disclosure of the health information to be used in the research from the individuals who are the subjects of the information **(section 50(1)a))**; and
- assess whether, in the opinion of the ethics committee,
    - the proposed research is of sufficient importance that the public interest in the proposed research outweighs to a substantial degree the public interest in protecting the privacy of the individuals who are the subjects of the health information to be used in the research;
    - the researcher is qualified to carry out the research;
    - adequate safeguards will be in place at the time the research will be carried out to protect the privacy of the individuals who are the subjects

of the health information to be used in the research and the confidentiality of that information; and
  - obtaining the consents referred to in **clause (a)** is unreasonable, impractical or not feasible. **(section 50(1)(b))**

Form of Consent

If an ethics committee determines under **section 50(1)(a)** that a researcher needs to obtain consents from individuals for the disclosure of their health information to be used in the research, the consent form should be approved by the committee and meet the committee's guidelines or standards for consent. Such guidelines may require that the consent:

- be typed on the letterhead of the institution or organization administering the consent;
- use plain language that lay persons will understand;
- include:
  - the purpose of the study;
  - a description of the types of information which the researcher requests to be released by the custodian;
  - the purposes for which the information is to be used;
  - the name and address of the individual(s) or organization authorized to receive the information;
  - the name and address of the individual (the personal health number and date of birth may be needed by certain custodians to identify the individual);
  - the time period during which the disclosure is authorized or remains valid;
  - a statement that the study participant holds the custodian (and its affiliates) harmless from any and all claims which may arise as a result of the disclosure of the information;
  - a confidentiality clause or statement that restricts access to the information to only certain persons (e.g. the researcher(s), the sponsor, Food and Drug Authority officials (if this is needed for pharmaceutical trials), the ethics committee auditors, etc.);
  - confirmation that the individual providing consent is 18 years of age or older;
  - spaces for the signatures of the study participant or his or her parent or guardian (if the participant is under 18 years of age) and a witness;
  - space for the study participant to identify the date of signature;
  - an acknowledgement that the study participant has been made aware of the reasons why the health information is needed and the risks and benefits to the individual of consenting or refusing to consent to the disclosure;
  - a statement that the consent may be revoked at any time; and
  - a statement that the information disclosed to the researcher will not be made available to any other party without further authorization and that the researcher will have adequate safeguards in place to protect the privacy of the study participants and the confidentiality of that information.

Assessment By Ethics Committee

The assessment that an ethics committee must undertake in **section 50(1)(b)** is stricter and broader than the privacy impact assessment (PIA) that custodians must undertake in **sections 64(1), 70, 71 and 46**. It is stricter because under **section 50(1)(b)(i),** the committee must form an opinion that the potential privacy – adverse impacts of the research are substantially outweighed by the public benefits expected from it. It is not enough for a researcher to be able to show how he or she would mitigate potential privacy impacts or that there would be some (or limited) public interest in the proposed research.

The assessment under **section 50** is also broader than a PIA because it includes an assessment of both the qualifications of the researcher as well as the practicality or reasonableness of obtaining consents from the study participants **(section 50(1)(b)(ii) and (iv))**.

Just as in PIAs, however, an important part of the assessment is whether the researcher will have adequate safeguards in place at the time the research will be carried out to protect the privacy of the individual subjects and the confidentiality of their health information **(section 50(10(b)(iii))**.

If data matching is performed for the purpose of conducting research, in addition to the requirements set out in **sections 48 to 56,** a custodian must carry out a PIA, meeting the requirements of **section 70(3) or 71(2)**.

For more information on privacy impact assessments, see section 5.2.8 (Duty to Prepare Privacy Impact Assessments) in Chapter 5 of this Publication. For more information on adequate safeguards for protection of the privacy and confidentiality of health information, see section 5.2.4 (Duty to Protect Health Information) in Chapter 5 of this Publication.

When making an assessment under **section 50(1)(b)** as to whether the public interest in the research outweighs to a substantial degree the public interest in protecting the privacy of study participants, an ethics committee must consider the degree to which the proposed research may contribute to:

- identification, prevention or treatment of illness or disease;
- scientific understanding relating to health;
- promotion and protection of the health of individuals and communities;
- improved delivery of health services; or
- improvements in health system management **(section 50(2))**.

Ethics committees follow the guidelines in the Tri-Council Policy Statement, as well as their own regulations or guidelines regarding conflict of interest as this applies to the research proposal. This enables them to consider the degree to which the researcher is independent from or motivated by vested commercial or other private interests.

An ethics committee may determine that it is unreasonable, impractical or not feasible to obtain consents to disclosure of the information from the study participants.

Some committees do not require consent for disclosure of health information when patients are not being contacted directly. This could occur when the research involves a chart review, or access to certain data (e.g. access to Cancer Registry data) or where a researcher has made a general request to members of the public to respond to a research questionnaire.

Response of Ethics Committee

Under **section 50(3)**, the ethics committee must prepare a response to the researcher setting out:

- its recommendation about obtaining consents from study participants under **section 50(1)(a)**;
- its assessment of the matters under **section 50(1)(b)** (public interest in research outweighing potential privacy impacts; qualifications of researcher; adequacy of safeguards to protect privacy and confidentiality; practicality, feasibility of obtaining consents); and
- any conditions that the committee considers should be imposed on the researcher.

A copy of the committee's response must be sent to the Information and Privacy Commissioner **(section 50(4))**. The notification of the Commissioner is intended to ensure that his office is kept aware of any potential impacts on individual privacy that may arise from the disclosure of individually identifying diagnostic, treatment and care information or registration information to be used for a research purpose.

This provision is not meant to create additional work for ethics committees. If the items in **section 50(3)** are included in the final approval letter to the researcher, providing a copy of that letter to the Commissioner would be sufficient.

If the ethics committee is not satisfied regarding any of the matters that were part of its assessment in **section 50(1)(b)**, the researcher may not apply to a custodian for disclosure of the health information **(section 51)**.

8.15.3 APPLICATION TO CUSTODIAN FOR DISCLOSURE FOR RESEARCH PURPOSE

If the ethics committee is satisfied with the assessment done under **section 50(1)(b)**, the researcher may forward to one or more custodians the response of the ethics committee and a written application for the health information to be used in the research **(section 52)**.

Even if a custodian has received an application from a researcher supported by a positive response from an ethics committee, the custodian can exercise its discretion not to disclose the health information applied for **(section 53(1)**.

If the custodian decides to disclose the health information:

- the custodian must impose on the researcher any conditions suggested by the ethics committee under **section 50(3)(c)**; and may impose other conditions on the researcher, as necessary; and
- the researcher must obtain the consents referred to in **section 50(1)(a)**, if recommended by the ethics committee, prior to the disclosure **(section 53(2))**.

8.15.4 AGREEMENT WITH RESEARCHER

Pursuant to **section 54(1)**, if a custodian decides to disclose health information to a researcher, the researcher must enter into an agreement with the custodian. The researcher must agree:

- to comply with the *Act* and the regulations, any conditions imposed by the custodian relating to the use, protection, disclosure, return or disposal of the health information, and any requirement imposed by the custodian to provide safeguards against identification, direct or indirect, of a subject individual;
- to use the health information only for the purpose of conducting the proposed research;
- not to publish the health information in a form that could reasonably enable the identify of an individual who is the subject of the information to be readily ascertained;
- not to make any attempt to contact an individual who is the subject of the health information to obtain additional health information unless the individual has provided the custodian with the consent referred to in **section 55;**
- to allow the custodian to access or inspect the researcher's premises to confirm that the researcher is complying with the *Health Information Act*, the Regulations, conditions and requirements in **section 54(1)(a);** and
- to pay the costs, if any, set by the custodian under **section 54(3)**.

"Readily ascertained" means that the individual's name or other identifiers or distinguishing characteristics associated with an individual can be determined or deduced without having to apply a sophisticated technical method or process, or without having the particular technical expertise to do so.

The identity of an individual can be said to be "readily ascertained" if:

- it can be determined by combining available data or information within the same or in several different records;
- it can be determined by comparing information representing distinguishing characteristics with other information sources having both the distinguishing characteristics and the names or other identifiers of individuals; and
- if only readily available or conventional computer hardware, software and technical expertise is used.

Where, for example, a pharmaceutical company is sponsoring clinical trial research, the custodian and sponsor will negotiate the arrangements for research in a separate agreement. A custodian may use an affiliate with hospital privileges to conduct the research. The Alberta Cancer Board often uses oncologists who have privileges with the Board to conduct patient trials of new cancer drugs.

Once the proposal for this type of research has been approved by the ethics committee, the custodian should enter into a research agreement with the affiliate(s) who is (are) conducting the sponsored research. Since an affiliate may conduct a number of sponsored clinical trial research projects for a custodian, it may be more efficient to have a form of master agreement signed in advance with each affiliate who will be conducting research. The master agreement would bind the researcher to the requirements of **section 54**. As each research proposal is approved by the ethics committee, the details of that particular research project, health information to be disclosed, security safeguards, access restrictions, etc. would be added to the affiliate's master agreement by way of a schedule.

See Appendix 4 of this Publication for the Components of a Research Agreement under Section 54. Custodians should seek legal advice in the drafting of any research agreement.

Custodians who are also public bodies under the *FOIP Act* should note that the research agreement requirements set out in **section 54(1)** are not the same as those set out in **section 40** of the *FOIP Act* and **section 8** of the *FOIP* Regulation which apply to disclosure of other types of personal information for research or statistical purposes.

Once the agreement in **section 54(1)** has been entered into, the custodian may disclose the requested health information to the researcher. The disclosure may be done with the consent of the individuals who are the subjects of the information, where that has been recommended by the ethics committee, or without the individuals' consent where obtaining consents has not been recommended **(section 54(2))**.
Under **section 54(3)**, the custodian may determine the costs of preparing information for disclosure; making copies of health information; and obtaining the consents required under **section 55**, if the researcher wishes to contact the subjects of the research. The costs must not exceed the actual cost of providing those services. The fees set out in the Fee Schedule under the Health Information Regulation do not apply to the costs determined by the custodian under this section.

8.15.5 CONSENT FOR ADDITIONAL INFORMATION

If the researcher wishes to contact the individuals who are the subjects of the information disclosed under **section 54(2)** to obtain additional health information, the custodian or one of its affiliates must first obtain consents from those individuals to their being contacted for that purpose **(section 55)**.

8.15.6 COURT ORDER

Under **section 54(1)(e)**, a researcher must agree to allow the custodian to access or inspect the researcher's premises to confirm that the researcher is complying with the *Act*, the regulations and the conditions and requirements in **54(1)(a)**. **Section 56(1)** provides that if a researcher refuses to allow a custodian to access or inspect its premises in accordance with the research agreement, the custodian may apply to the Court of Queen's Bench by notice of motion for an order to enforce compliance with the research agreement.

If the Court is satisfied that there are reasonable and probable grounds to believe that access to premises or the production or removal of documents is necessary for the purpose of determining whether the research agreement is being complied with, the Court may make any order it considers necessary to enforce compliance with the agreement **(section 56(2))**.

An order under **section 56(2)** may authorize a custodian to:

- enter and search any premises of the researcher where the research is conducted;
- operate or cause to be operated any computer system of the researcher to search any data contained in or available to the system and produce a document from the data; and
- seize and make copies of any documents of the researcher that are or may be relevant to the investigation.
(section 56(3))

"Document" is defined in **section 56(6)** to include any correspondence, memorandum, book, plan, map, drawing, diagram, pictorial or graphic work, photograph, film, microfilm, sound recording, videotape, machine readable record or other material or thing, regardless of physical form or characteristics.

An application for an order under this section may be made ex parte unless the Court orders otherwise **(section 56(5))**. **"Ex Parte"** means that the notice of motion does not have to be served on the researcher and the order can be obtained in the absence of the researcher **(section 56(4))**. The Court may decide that providing notice of the application to the researcher may not be expedient under the circumstances or that it would enable the researcher to modify or destroy evidence needed for the investigation.

Any documents seized by the custodian pursuant to a court order must be returned to the researcher within 60 days after the conclusion of the investigation, including any hearing or appeal **(section 56(5))**.

THINGS TO REMEMBER

DISCLOSURE OF HEALTH INFORMATION

- A custodian must not disclose health information except in accordance with the *Health Information Act.*
- A custodian may disclose non-identifying health information to anyone for any purpose but must inform a non-custodian that the Commissioner must be notified if the recipient intends to use the information for data matching.
- A custodian must disclose the least amount of health information at the highest level of anonymity possible unless the disclosure is for providing health services or for determining the individual's eligibility to receive a health service.
- A custodian must consider any expressed wishes of the individual who is the subject of the information and any other factors the custodian considers relevant in deciding how much health information to disclose.
- An affiliate must only disclose the health information necessary to carry out his/her responsibilities as assigned by the custodian.
- A custodian may only disclose non-recorded individually identifying health information for the purpose for which the information was provided to the custodian.
- A custodian must make a reasonable effort to ensure that the person to whom the disclosure is made is the person intended and authorized to receive the information.
- When a custodian discloses a record containing individually identifying diagnostic, treatment and care information without consent, including disclosure to another custodian, the disclosing custodian must make a notation of the name of the recipient, the date and purpose of the disclosure and a description of the information disclosed. The disclosure notation may be in paper or electronic form, may be put on the individual's health or drug record or in a book or "disclosure log". The notation must be kept for 10 years.
- A custodian that discloses individually identifying diagnostic, treatment and care information must inform the recipient in writing of the purpose for the disclosure and the custodian's authority for disclosing the information (see Notices to Recipients (section 42)).

- If a custodian intends to disclose individually identifying diagnostic, treatment and care information by electronic means, the custodian must first obtain the individual's consent to the means of disclosure (section 59) or ensure that consent has been previously obtained. No consent is required if the disclosure is for processing payment for a health service.
- A custodian may refuse to disclose individually identifying health information without consent under sections 35, 36, 37, 38 and 40.
- A custodian must disclose individually identifying health information to the Minister or the Department if the information is requested for health system purposes (section 46) and the authority for the request is from another statute or relates to a health service funded by the department. However, if the information requested relates to a health service funded by the department, the department must first prepare a Privacy Impact Assessment and submit it to the Commissioner for review and comment.
- Before disclosing the information obtained from another custodian for health system purposes to regional health authorities, the Alberta Mental Health Board or the Alberta Cancer Board, the department must also consider the comments of the Commissioner made in response to the Privacy Impact Assessment.
- A custodian must disclose individually identifying health information to a regional health authority, the Alberta Mental Health Board or the Alberta Cancer Board if the authority for the request is from another statute. A custodian may refuse to disclose individually identifying health information to a regional health authority, the Alberta Mental Health Board or Alberta Cancer Board for health system purposes (under section 47) if the authority for the request is because the disclosing custodian is receiving funding for the health service from the requesting custodian. However, the disclosing custodian must provide the requesting custodian with non-identifying health information and the requesting custodian may ask the Commissioner to review the refusal.

To Whom May a Custodian Disclose Individually Identifying Diagnostic, Treatment and Care Information to?

- The individual who is the subject of the information or to an authorized representative of the individual;
- If the custodian has the individual's consent, he/she may disclose the individual's identifying diagnostic, treatment and care information to anyone (see 'Some Things to Remember About Consent', the forms for

consent under section 34(2) and section 59 in Appendix 1 of the Manual and also Chapter 8 of the Manual)

- If the custodian does not have the individual's consent, he/she may disclose the individual's identifying diagnostic, treatment and care information, subject to the rules in the *Act* regarding the least amount of information at the highest degree of anonymity, to:

  - any other custodian for purposes authorized by section 27 of the *Act* (see 'Some Things to Remember about Use' – Authorized Purposes and Chapter 7 of the Manual);
  - any person who is responsible for providing continuing treatment and care to the individual;
  - other persons for the purposes listed in section 35 of the *Act*;
  - the Provincial Archives of Alberta or to an archives that is subject to the *Health Information Act* or to the *FOIP Act* for permanent preservation and historical research;
  - the Minister if, in the custodian's opinion, the disclosure is necessary or desirable to enable the Minister to carry out the duties of the Minister;
  - the Minister, the department, the Alberta Cancer Board, the Alberta Mental Health Board or a regional health authority for health system purposes (sections 46, 47);
  - To a researcher for a research purpose if the rules in sections 49 to 56 are complied with (see Section 8.16 in Chapter 8 of the Manual).

To Whom May a Custodian Disclose Individually Identifying Registration Information to?

- The individual who is the subject of the information or to an authorized representative of the individual;
- If the custodian has the individual's consent, he/she may disclose the individual's individually identifying registration information to anyone (See 'Some things to Remember About Consent', the forms for Consent under Section 34 and Section 59 in Appendix 1 of the Manual and also Chapter 8 of the Manual);
- If the custodian does not have the individual's consent, he/she may disclose the individual's individually identifying registration information, subject to the rules in the *Act* regarding the least amount of information at the highest degree of anonymity, to:

  - any other custodian for purposes authorized by section 27 of the *Act* (see 'Some Things to Remember about Use' – Authorized Purposes and Chapter 7 of the Manual);
  - certain other recipients for the purposes listed in section 36 of the *Act*
  - ambulance operators and ambulance attendants (authorized under the Health Information Regulation);
  - the Provincial Archives of Alberta or to an archives that is subject to the *Health Information Act* or to the *FOIP Act* for permanent preservation and historical research;
  - the Minister if, in the custodian's opinion, the disclosure is necessary or desirable to enable the Minister to carry out the duties of the Minister;
  - the Minister, the Department, the Alberta Cancer Board, the Alberta Mental Health Board or a regional health authority for health system purposes (sections 46, 47);
  - To a researcher for a research purpose if the rules in section 49 to 56 are complied with (see Section 8.16 in Chapter 8 of this Publication).

To Whom May a Custodian Disclose Individually Identifying Health Services Provider Information to?

- The individual who is the subject of the information or to an authorized representative of the individual;
- If the custodian has the individual's consent, he/she may disclose the individual's individually identifying health services provider information to anyone (See 'Some things to Remember About Consent', the forms for Consent under Section 34 and Section 59 in Appendix 1 of the Manual and also Chapter 8 of the Manual);
- If the custodian does not have the individual's consent, he/she may disclose the individual's individually identifying health services provider information, subject to the rules in the *Act* regarding the least amount of information at the highest degree of anonymity, to:

  - a health professional body that requests the information for the purposes of an investigation, discipline proceeding, practice review or an inspection relating to the health services provider;
  - persons listed in section 37 of the *Act*;
  - anyone, providing the information disclosed is: name, business address and telephone number, type of health service provider, profession, job classification, employer and municipality where the

practice is located of the health services provider and the disclosure will not reveal other information or reasonably be expected to result in mental, physical or undue financial harm to the health services provider;

- the Provincial Archives of Alberta or to an archives that is subject to the *Health Information Act* or to the *FOIP Act* for permanent preservation and historical research;
- the Minister if, in the custodian's opinion, the disclosure is necessary or desirable to enable the Minister to carry out the duties of the Minister;
- the Minister, the Department, the Alberta Cancer Board, the Alberta Mental Health Board or a regional health authority for health system purposes (sections 46, 47).

FUNDAMENTALS OF CONSENT

When is Consent under Section 34(2) Required?

Consent under this section is normally required whenever a custodian discloses individually identifying health information (i.e. diagnostic, treatment and care information, registration information or health services provider information) outside of the "controlled arena" to non-custodians. Examples of requests for disclosure where consent would be required include disclosure to an insurance company, to an employer or to a physician providing services to the Workers' Compensation Board. (See the form for Consent under section 34(2)).

Requirements for Consent under Section 34(2)

- Must be provided in writing or electronically;
- Must include:
  - authority for the custodian to disclose the health information specified in the consent;
  - the purpose for which the health information may be disclosed;
  - the identify of the person to whom the information is to be disclosed;
  - an acknowledgement that the individual has been made aware of the reasons why the health information is needed and the risks and benefits of consenting or refusing to consent;
  - the date the consent is effective and the date, if any, on which the consent expires; and
  - a statement that the consent may be revoked at any time.
- Revocation of consent must be provided in writing or electronically.
- Consent or revocation of consent must be signed by the person providing it.

When is Consent under Section 34(2) Not Required?

Consent is not required when a custodian discloses individually identifying health information to other custodians for authorized purposes (see section 27 of the *Act*) (see 'Some Things to Remember About Use' – Authorized Purposes and Chapter 7 of the Manual).

Consent is not required when a custodian is disclosing information outside the "controlled arena" in accordance with the following exceptions: (Note that a custodian may still exercise discretion in disclosing individually identifying health information under sections 35, 36, 37, 38 and 40)

- Disclosure of individually identifying diagnostic, treatment and care information to the persons and under the conditions listed in section 35 of the *Act:*
  - ☐ **To a person responsible for providing continuing treatment and care to the individual (section 35(1)(b))**
  - ☐ **To a family member or another person with whom the individual is believed to have a close personal relationship if the information is given in general terms and concerns the presence, location, condition, diagnosis, progress and prognosis of the individual on the day on which the information is disclosed and the individual has not requested otherwise (section 35(1)(c))**
  - ☐ **To inform family members of the individual, or a person with whom the individual is believed to have a close personal relationship, that the individual has been injured, is ill or has died if the individual has not requested otherwise (section 35(1)d))**
  - ☐ **To an official of a penal or other custodial institution in which the individual is being lawfully detained for the purpose of providing health services to the individual (section 35(1)(e))**
  - ☐ **To a person authorized to conduct an audit of the information if the person enters into an agreement with the custodian about non-disclosure and destruction of the information (section 35(1)(f))**
  - ☐ **To a quality assurance committee to carry out quality assurance activities within the meaning of section 9 of the Alberta Evidence Act (section 35(1)(g))**
  - ☐ **To provide information for a court proceeding or a proceeding before a quasi-judicial body (section 35(1)(h) (Note – the custodian must be a party to the proceeding)**
  - ☐ **To comply with a subpoena, warrant or court order compelling the production of information or with a rule of court that relates to the production of information (section 35(1)(i)) (Note: the body issuing the warrant or order must have jurisdiction to compel the production of information)**

- ☐ **To investigate an offence involving a life-threatening personal injury to the individual if the individual has not requested otherwise (section 35(1)(j) (Note – the person receiving the information under this provision can be a member of a municipal, provincial or first nations police service)**

- ☐ **To another custodian to detect or prevent fraud, limit abuse in the use of health services or prevent the commission of an offence under an enactment of Alberta or Canada (section 35(1)(k))**

- ☐ **To enable an officer of the Legislature (e.g. Auditor General, Ombudsman, Chief Electoral Officer, Information and Privacy Commissioner) to carry out his/her duties (section 35(1)(l))**

- ☐ **To any person to avert or minimize an imminent danger to the health or safety of any person (section 35(1)(m))**

- ☐ **To act in the best interests of the above individual if the individual lacks the mental capacity to provide consent (section 35(1)(n))**

- ☐ **To a descendant of a deceased individual, to a representative under section 104(1)(c) to (i) or to a person providing health services to the descendant (section 35(1)(o)) (Note – the disclosure must be necessary to provide health services to the descendant and the privacy of the deceased individual must be protected)**

- ☐ **To comply with another act or regulation of Alberta or Canada that authorizes or requires the disclosure (section 35(1)(p))**

- ☐ **To transfer records to a successor custodian because the first custodian is ceasing to be a custodian (section 35(1)(q))**

- ☐ **To enable a health professional body to conduct an investigation, a discipline proceeding, a practice review or an inspection (section 35(4)) (Note—the custodian must comply with other relevant legislation and the health professional body must enter into an agreement with the custodian about non-disclosure and destruction of the information)**

- Disclosure of individually identifying registration information to the persons and under the conditions listed in section 36 of the *Act*:

  - ☐ **For any purpose for which diagnostic, treatment and care information may be disclosed under section 35(1) or (4) (section 36(a))**

  - ☐ **To any person for collecting or processing a fine or debt owing by the individual to the Government of Alberta or to a custodian (section 36(b))**

  - ☐ **To an ambulance attendant or operator under the *Ambulance Services Act*) (section 36(c))**

- Disclosure of individually identifying health services provider information to the persons and under the conditions listed in section 37 of the *Act*:
  - ☐ **To a health professional body for the purpose of an investigation, discipline proceeding, practice review or inspection relating to the health services provider (section 37(1)(a))**
  - ☐ **To comply with an enactment of Alberta or Canada that authorizes or requires the disclosure (section 37(1)(b))**
  - ☐ **"Business card" information to any person for any purpose unless the disclosure would reveal other information abut the provider or could reasonably be expected to result in harm to the mental or physical health or safety of the provider or undue financial harm to the provider**

  Rules regarding the disclosure of health services provider information by the regulatory bodies of the health profession are generally found in their governing health professional statute (e.g. *Medical Profession Act, Nursing Profession Act, Pharmaceutical Profession Act* or in the *Health Professions Act,* when it is proclaimed in force for each of the various health professions subject to it.

- Disclosure of individually identifying health information to an archives for permanent preservation and historical research (section 38 of the *Act*);

- Disclosure of individually identifying health information to the Minister if it is necessary or desirable in the custodian's opinion to enable the Minister to carry out his duties (section40);

- Disclosure to the Minister, the Department, a regional health authority, Alberta Mental Health Board or Alberta Cancer Board if the information is requested for health system purposes (section 46 and 47). A custodian may not refuse to disclose individually identifying health information to the above bodies if the authority for the request is from another statute (e.g. *Cancer Programs Act, Public Health Act*). A custodian may refuse to disclose individually identifying health information to regional health authorities, Alberta Mental Health Board or Alberta Cancer Board if the only authority for the request is because the custodian is receiving funding from that body (however, the disclosing

custodian must still provide non-identifying health information to the requesting custodian and the requesting custodian may ask the Commissioner to review the refusal).

When is Disclosure Without Consent Authorized or Required under Section 35(1)(p)?

Some examples of other statutes that authorize or require the disclosure or certain types of individually identifying health information are:

- ☐ ***Criminal Code(Canada)*** **– provides indirect authority to compel disclosure of information as specified in warrants or subpoenas;**
- ☐ ***Fatality Inquiries Act*** **– requires custodians to report unexpected deaths to a medical examiner;**
- ☐ ***Protection for Persons in Care Act*** **– requires custodians to report on the possible abuse of an adult in care;**
- ☐ ***Child Welfare Act*** **- requires custodians to report on the possible abuse of a child; and**
- ☐ ***Public Health Act*** **– requires custodians to notify the Medical Officer of Health regarding certain communicable diseases and provides for the disclosure of information on recalcitrant patients.**

Other Considerations Regarding Consent

- Custodians need to be cautious about disclosing individually identifying health information (any of the three types) if there is a reasonable expectation of harm resulting to the individual.
- If a custodian so chooses, he/she may choose to obtain the individuals' consent prior to disclosing information to custodians inside the controlled arena or to persons outside of the controlled arena that are listed in sections 35, 36, 37, 38 of the Act even though there is no requirement to obtain consent in these instances.
- When there is a need to obtain consent from an individual who is under the age of 18 years or from an individual who is over the age of 18 years but who may be cognitively impaired, custodians must apply their clinical

judgment to determine whether the individual understands and appreciates the nature and consequences of providing or not providing their consent. If the individual cannot understand and appreciate the nature and consequences of providing or not providing their consent, the consent of a parent, guardian or other authorized representative of the individual (section 104(1)(c) to (i)) must be obtained.

- Consent from a parent or guardian obtained for a child under the age of 18 years would not remain valid for an individual once they are over the age of 18 years and a new consent would need to be obtained from the individual.

- Consent from a parent or guardian or from the individual him or herself (if over the age of 18 years) would need to be obtained from or for each member of a family. One consent covering all members of a family would not be sufficient.

When is Consent under Section 59 Required?

Section 59 requires that a custodian obtain consent or ensure that consent has been previously obtained from an individual before disclosing individually identifying diagnostic, treatment and care information by "electronic means". "Electronic means" is defined in section 1(2) of the *Health Information Act* Regulation as "a computer system that facilitates access by authorized persons to electronic or digital information that is stored in a computer database by a custodian".

What Must Be Included in Consent Under Section 59?

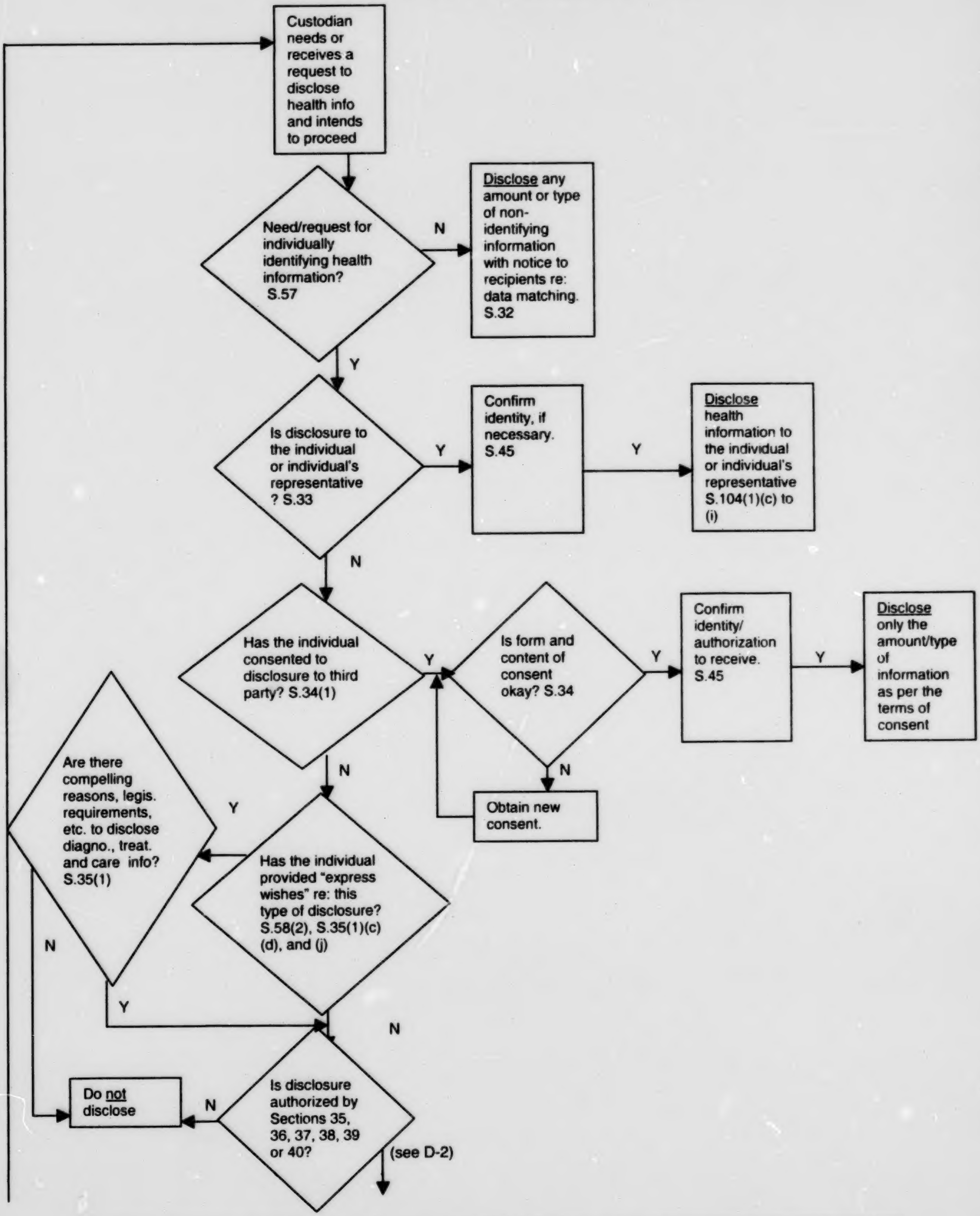
- Authority for any custodian to disclose individually identifying diagnostic, treatment and care information about the individual by electronic means for all the section 27 authorized purposes.
- Acknowledgment that the individual has been made aware of the reasons for disclosure by electronic means and the risks and benefits to the individual of consenting or refusing to consent.
- The date the consent is effective.
- A statement that the consent may be revoked at any time by the individual.

- The consent or revocation of consent must be in writing or provided electronically. If the consent is written, it must be signed by the person providing it.

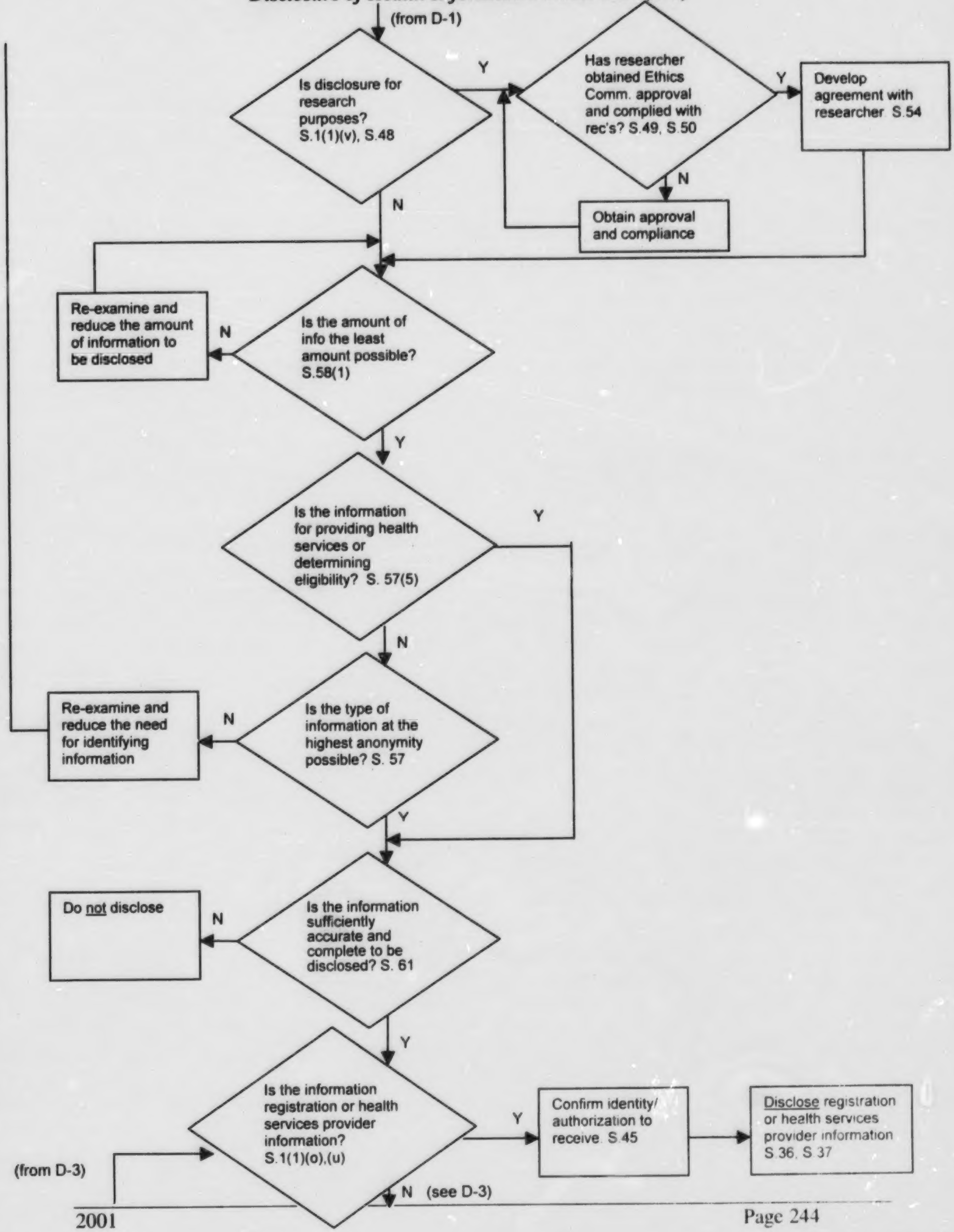
When is Consent under Section 59 Not Required?

Consent under this section is not required when the disclosure by electronic means is for the purpose of obtaining or processing payment for health services (e.g. if a pharmacist discloses information to a third party insurer or drug plan carrier for billing or claims payment purposes) (section 59(7)).

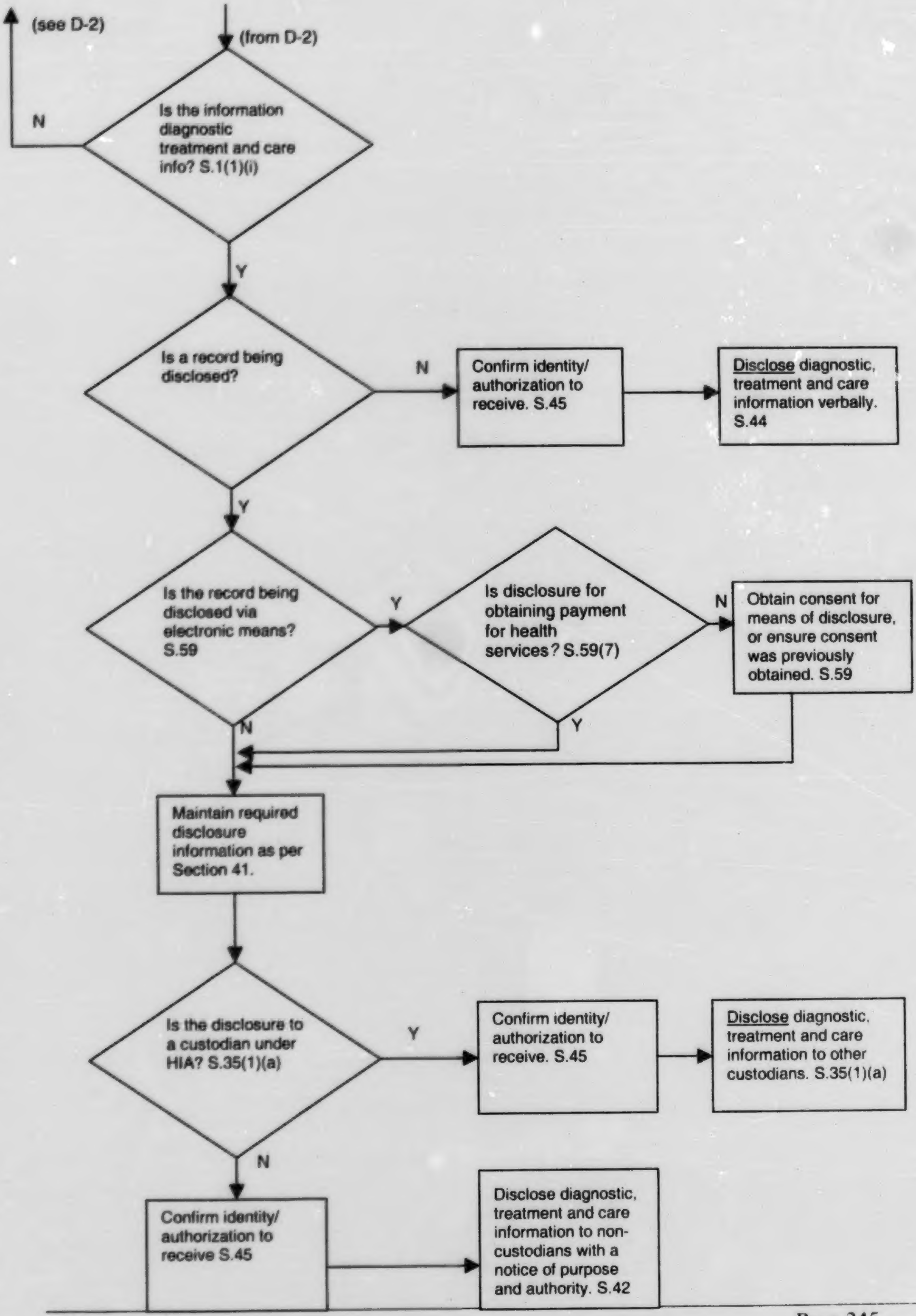
Disclosure of Health Information Under HIA (D-1)


Custodian needs or receives a request to disclose health info and intends to proceed
Need/request for individually identifying health information? S.57
N
Disclose any amount or type of non-identifying information with notice to recipients re: data matching. S.32
Y
Is disclosure to the individual or individual's representative ? S.33
Y
Confirm identity, if necessary. S.45
Y
Disclose health information to the individual or individual's representative S.104(1)(c) to (i)
N
Has the individual consented to disclosure to third party? S.34(1)
Y
Is form and content of consent okay? S.34
Y
Confirm identity/ authorization to receive. S.45
Y
Disclose only the amount/type of information as per the terms of consent
N
Obtain new consent.
N
Has the individual provided "express wishes" re: this type of disclosure? S.58(2), S.35(1)(c) (d), and (j)
Y
Are there compelling reasons, legis. requirements, etc. to disclose diagno., treat. and care info? S.35(1)
N
Y
N
Is disclosure authorized by Sections 35, 36, 37, 38, 39 or 40?
N
Do not disclose
(see D-2)

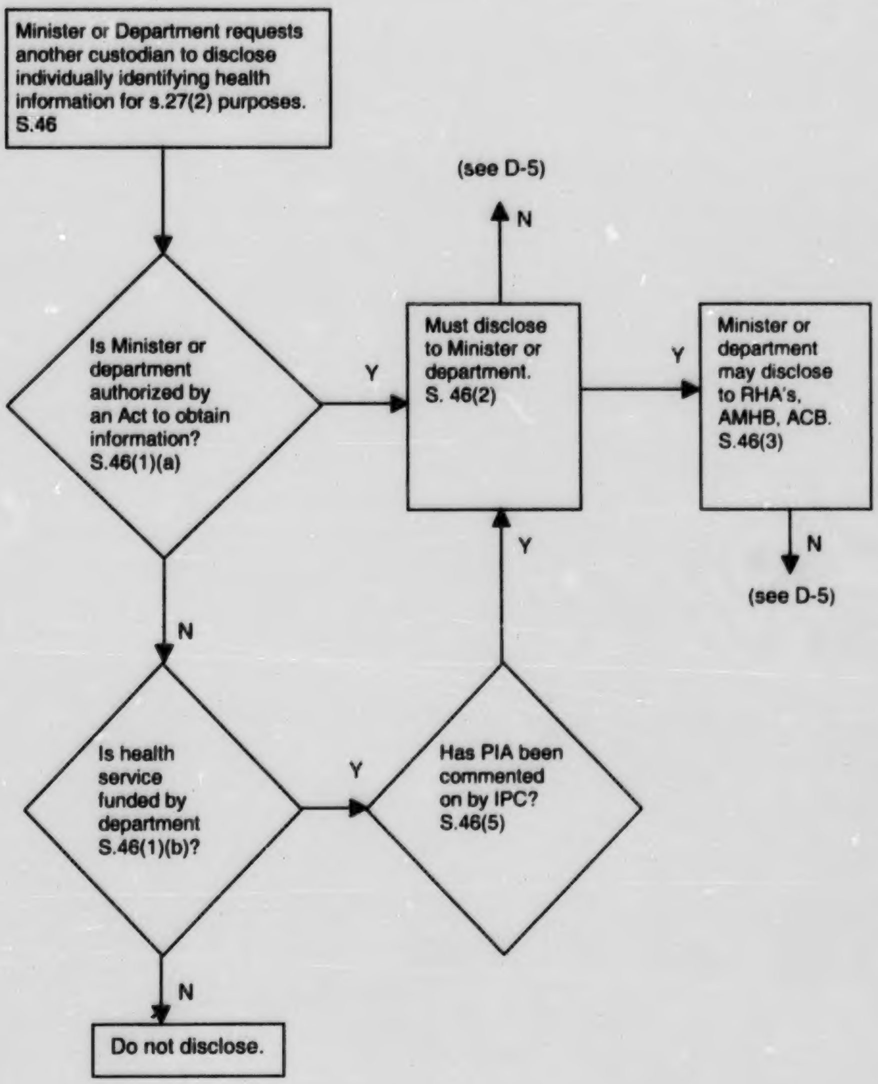
Disclosure of Health Information Under HIA (D-2)

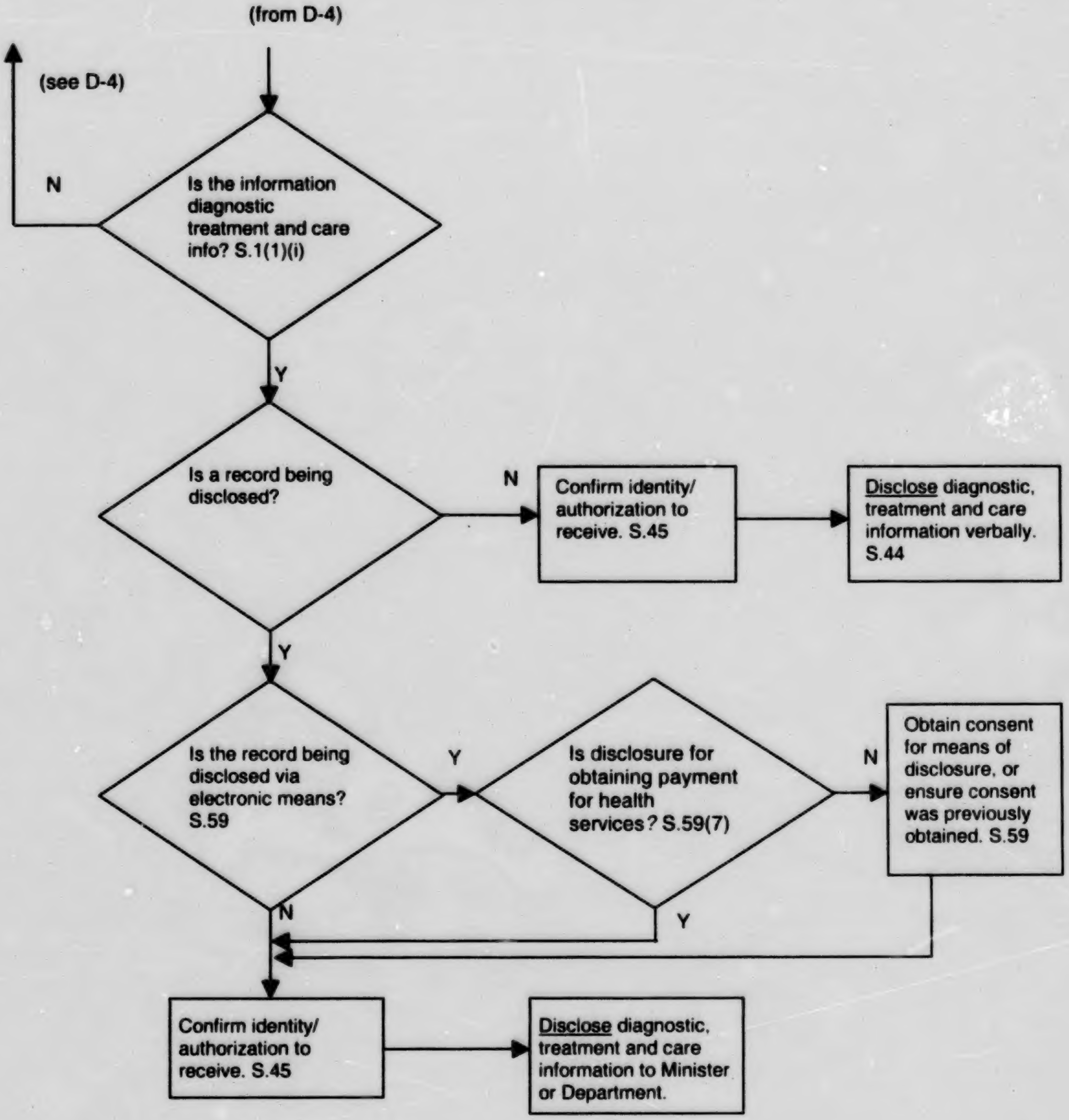

(from D-1)
Is disclosure for research purposes? S.1(1)(v), S.48
Y
Has researcher obtained Ethics Comm. approval and complied with rec's? S.49, S.50
Y
Develop agreement with researcher. S.54
N
Obtain approval and compliance
N
Re-examine and reduce the amount of information to be disclosed
N
Is the amount of info the least amount possible? S.58(1)
Y
Is the information for providing health services or determining eligibility? S. 57(5)
Y
N
Re-examine and reduce the need for identifying information
N
Is the type of information at the highest anonymity possible? S. 57
Y
Do not disclose
N
Is the information sufficiently accurate and complete to be disclosed? S. 61
Y
Is the information registration or health services provider information? S.1(1)(o),(u)
Y
Confirm identity/ authorization to receive. S.45
Disclose registration or health services provider information S.36, S.37
(from D-3)
N (see D-3)

Disclosure of Health Information Under HIA (D-3)

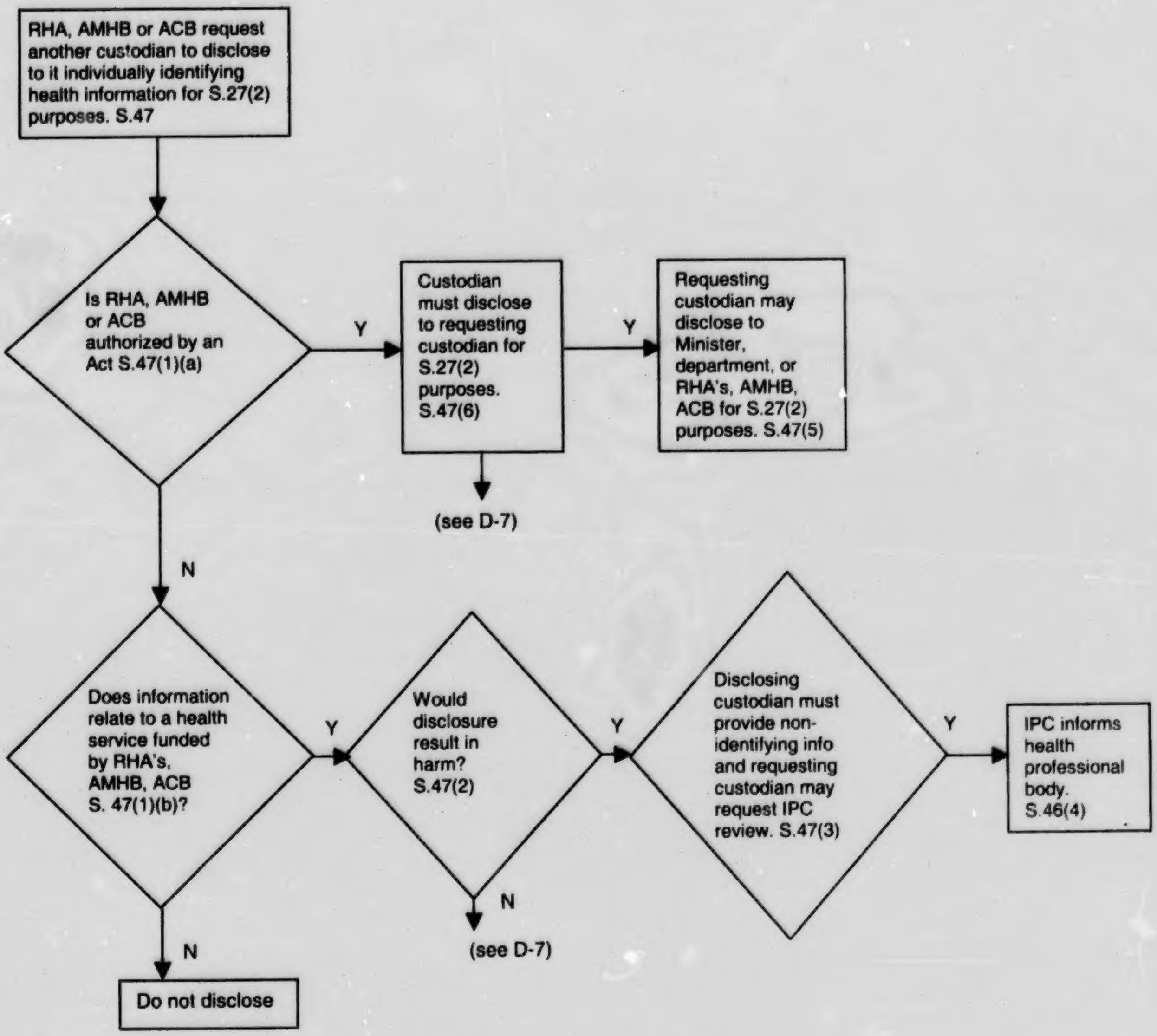

(see D-2)
(from D-2)
N
Is the information diagnostic treatment and care info? S.1(1)(i)
Y
Is a record being disclosed?
N
Confirm identity/ authorization to receive. S.45
Disclose diagnostic, treatment and care information verbally. S.44
Y
Is the record being disclosed via electronic means? S.59
Y
Is disclosure for obtaining payment for health services? S.59(7)
N
Obtain consent for means of disclosure, or ensure consent was previously obtained. S.59
Y
N
Maintain required disclosure information as per Section 41.
Is the disclosure to a custodian under HIA? S.35(1)(a)
Y
Confirm identity/ authorization to receive. S.45
Disclose diagnostic, treatment and care information to other custodians. S.35(1)(a)
N
Confirm identity/ authorization to receive S.45
Disclose diagnostic, treatment and care information to non-custodians with a notice of purpose and authority. S.42

Disclosure of Health Information for Health System Purposes (section 46) - (D-4)

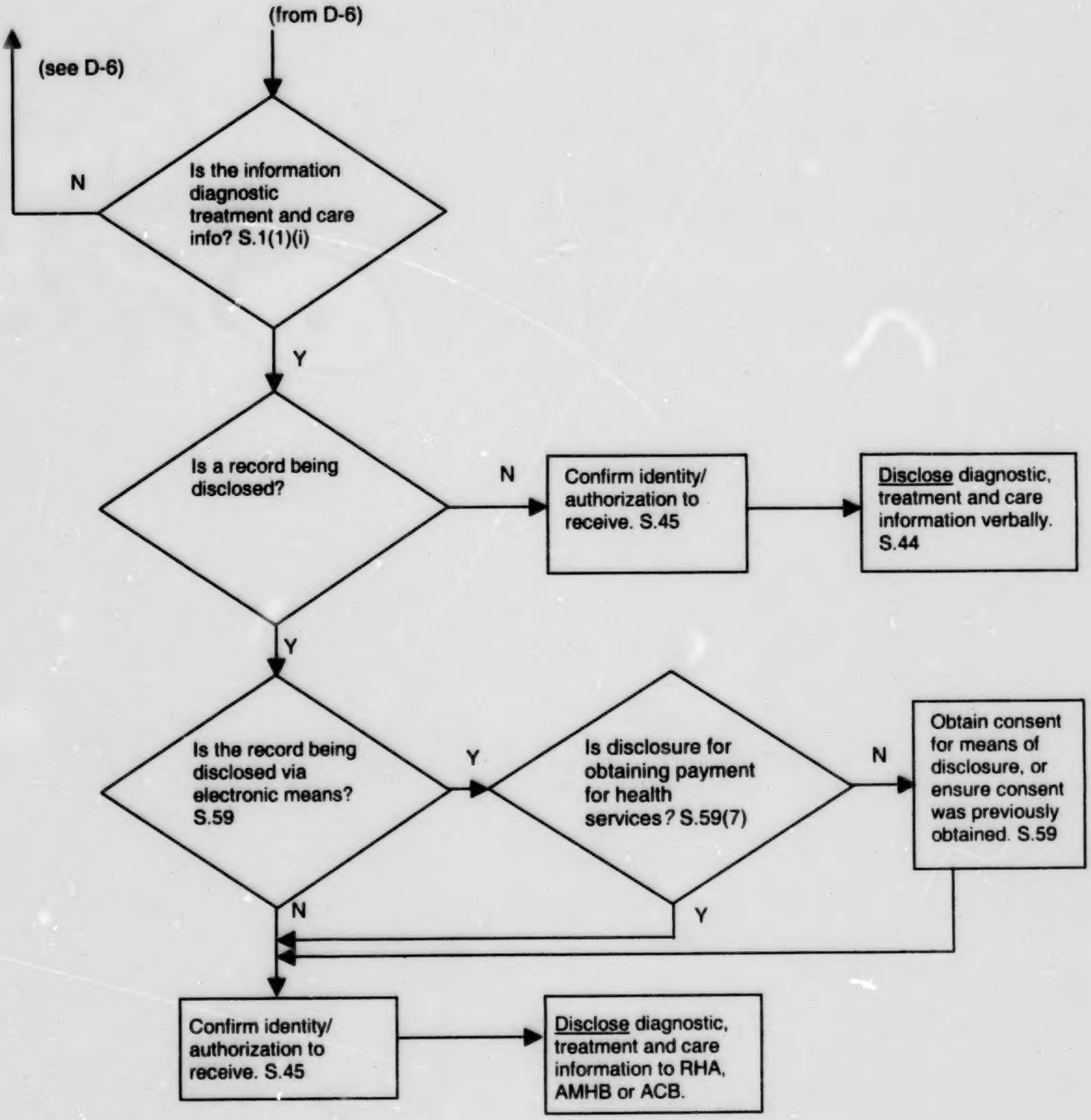

Minister or Department requests another custodian to disclose individually identifying health information for s.27(2) purposes. S.46
Is Minister or department authorized by an Act to obtain information? S.46(1)(a)
Y
N
Must disclose to Minister or department. S. 46(2)
(see D-5)
N
Y
Minister or department may disclose to RHA's, AMHB, ACB. S.46(3)
N
(see D-5)
Y
Is health service funded by department S.46(1)(b)?
Y
Has PIA been commented on by IPC? S.46(5)
N
Do not disclose.


(from D-4)
(see D-4)
N
Is the information diagnostic treatment and care info? S.1(1)(i)
Y
Is a record being disclosed?
N
Confirm identity/ authorization to receive. S.45
Disclose diagnostic, treatment and care information verbally. S.44
Y
Is the record being disclosed via electronic means? S.59
Y
Is disclosure for obtaining payment for health services? S.59(7)
N
Obtain consent for means of disclosure, or ensure consent was previously obtained. S.59
N
Y
Confirm identity/ authorization to receive. S.45
Disclose diagnostic, treatment and care information to Minister or Department.

Disclosure of Health Information for Health System Purposes (section 47) - (D-6)


RHA, AMHB or ACB request another custodian to disclose to it individually identifying health information for S.27(2) purposes. S.47
Is RHA, AMHB or ACB authorized by an Act S.47(1)(a)
Y
Custodian must disclose to requesting custodian for S.27(2) purposes. S.47(6)
Y
Requesting custodian may disclose to Minister, department, or RHA's, AMHB, ACB for S.27(2) purposes. S.47(5)
(see D-7)
N
Does information relate to a health service funded by RHA's, AMHB, ACB S. 47(1)(b)?
Y
Would disclosure result in harm? S.47(2)
Y
Disclosing custodian must provide non-identifying info and requesting custodian may request IPC review. S.47(3)
Y
IPC informs health professional body. S.46(4)
N
(see D-7)
N
Do not disclose

Disclosure of Health Information for Health System Purposes (section 47) - (D-7)


(from D-6)
(see D-6)
N
Is the information diagnostic treatment and care info? S.1(1)(i)
Y
Is a record being disclosed?
N
Confirm identity/ authorization to receive. S.45
Disclose diagnostic, treatment and care information verbally. S.44
Y
Is the record being disclosed via electronic means? S.59
Y
Is disclosure for obtaining payment for health services? S.59(7)
N
Obtain consent for means of disclosure, or ensure consent was previously obtained. S.59
N
Y
Confirm identity/ authorization to receive. S.45
Disclose diagnostic, treatment and care information to RHA, AMHB or ACB.

CHAPTER NINE

ADMINISTRATION OF THE ACT

9.1 OVERVIEW OF CHAPTER NINE

This Chapter will cover:

- the roles and responsibilities of custodians, affiliates, health professional bodies, the Department and the Information and Privacy Commissioner;
- the tasks and issues that custodians need to address to prepare to implement the *Act;*
- the identification of affiliates;
- the establishment or adoption of policies and procedures;
- the designation of (a) responsible affiliate(s), such as a Health Information Coordinator, and the coordinator's roles and responsibilities;
- the roles and responsibilities of the health records management function and the information management function;
- how notice is given under the *Act;*
- protection from liability; and
- penalties and sanctions under the *Act.*

9.2 ROLES AND RESPONSIBILITIES

9.2.1 CUSTODIANS

Custodians **(as defined in section 1(1)(f))** as the "gatekeepers" of health information, are responsible for maintaining, protecting and safeguarding health information in their custody or under their control. They are also responsible for safeguarding health information when it is transmitted or transported to other custodians or others outside the controlled arena, including transmission or transport outside the province.

See 'How the Act Works' in Section 1.3.2 of Chapter 1 and the definition of Custody and Control in 'To Whom Does the *Health Information Act* Apply?' in section 1.4.2 in Chapter 1 of this Publication.

In preparing to implement the *Act,* each custodian should establish internal processes and procedures suited to the organization's size, structure, specific circumstances and anticipated workload. A custodian's responsibilities under the *Act* include:

- receiving and responding to requests for health information, meeting the duty to assist applicants and collecting any fees as set out in the *Act* **(sections 7-10, 12, 15, 17 and 67)**;
- deciding what information will be released and what information will be excepted from disclosure under the legislation **(section 11)**;
- receiving and responding to requests for correction or amendment **(sections 13-15)**;
- fulfilling the various duties of the custodian relating to the collection, use and disclosure of health information, including the rules regarding the least amount of information and the highest degree of anonymity **(sections 18-72)**;
- responding to the Information and Privacy Commissioner to resolve requests for reviews and complaints under the *Act* **(sections 73-82, 84, 85)**;
- assisting the public by designating one or more individuals to be responsible for

the implementation and administration of the *Act;* and
- making available any policies and procedures regarding the implementation of the *Act* **(sections 62 and 63)**.

9.2.2 AFFILIATES

"Affiliates" as defined in **section 1(1)(a)** must comply with the *Act* and Regulations, and any policies and procedures established or adopted under **section 63**.

Any collection, use or disclosure of health information by an affiliate is considered to be a collection, use or disclosure by the custodian **(section 62)**. Any disclosure of health information to an affiliate is considered to be a disclosure to the custodian. Although affiliates of a custodian must comply with the *Act,* the regulations and the custodian's policies and procedures, the custodian remains ultimately responsible for compliance under the *Health Information Act.*

9.2.3 HEALTH PROFESSIONAL OR OTHER REGULATORY BODIES

Bodies that regulate the practice of health professionals such as the College of Physicians and Surgeons of Alberta, the Alberta Association of Registered Nurses as well as associations of individual custodians, such as the Provincial Health Authorities of Alberta, the Alberta Medical Association and the Alberta College of Pharmacists, are not custodians.

Representatives of many of these organizations were involved in working groups assisting Alberta Health and Wellness with the development of the regulations under the *Act* and as members of the *Health Information Act* Implementation Steering Committee. These bodies may retain a continuing role in assisting their members in interpreting and applying the *Act* relevant to their sector.

9.2.4 MINISTER RESPONSIBLE FOR THE *HEALTH INFORMATION ACT*

The Lieutenant Governor in Council designates the Minister Responsible for the *Act* by Order in Council. The Minister of Alberta Health and Wellness has been given this responsibility.

The Minister has overall responsibility for the general administration of the *Act* across the province, including preparing and submitting amendments to the *Act* and the Regulations.

9.2.5 ALBERTA HEALTH AND WELLNESS

The department of Alberta Health and Wellness supports the Minister in all aspects of implementing and administering the legislation across all custodians.

The department is responsible for overall leadership and direction in communicating with the public about implementation of the *Act.*

The department is also responsible for the overall leadership and direction of training activities related to the implementation of the *Act,* including the development of training delivery media and infrastructure to support initial training.

The department will provide the following services and products to custodians:

- help desk support services, particularly to custodians providing a single health service or who work in a clinic to assist in the application and explanation of the *Act*;
- samples of communications templates such as newsletters, brochures and posters, developed in consultation with custodians and various organizations;
- training and awareness materials for custodians to deliver to their staff and training courses for persons designated as responsible for the implementation and administration of the *Act;* and
- updates to this Manual as the *Act* is interpreted through orders from the Commissioner.

9.2.6 INFORMATION AND PRIVACY COMMISSIONER

The Information and Privacy Commissioner is an Officer of the Legislature who is independent from government. The Commissioner is responsible for reviewing decisions of custodians and affiliates under the *Act;* conducting investigations; providing advice; and resolving disputes.

The Commissioner must report annually to the Speaker of the Legislative Assembly on the work of the Commissioner's Office and such other matters relating to the protection of health information as the Commissioner considers appropriate.

The duties, powers and responsibilities of the Commissioner and the role of the Commissioner's Office are set out in **Part 7** of the *Act* and in **Chapter 10 of this Publication**.

9.3 IDENTIFYING RESPONSIBLE AFFILIATES

Section 62 requires each custodian to identify its affiliates who will be responsible for ensuring compliance with the *Act*, the regulations and the policies and procedures established or adopted by the custodian under **section 63**. Carrying out this requirement would include designating a person who will have overall responsibility for ensuring compliance with the *Health Information Act* (i.e. a responsible affiliate or Health Information Coordinator, in some organizations).

According to the definition of **"affiliate"** in **section 1(1)(a),** the affiliates identified would be the custodian's employees; those providing a service to or for the custodian such as contractors, agents, individuals appointed to committees, volunteers or students; and health service providers with hospital privileges (for custodians that operate hospitals under the *Hospitals Act).*

9.4 *HEALTH INFORMATION ACT* IMPLEMENTATION

The following issues and tasks need to be addressed by each custodian before the *Act* comes into effect.

The following is a summary of the more detailed *Health Information Act* Implementation Checklist in Appendix 3 of this Publication.

1. **Establish a Structure Necessary to Administer the Act.**

- **Designate (a) responsible person(s)**

Custodians have a number of responsibilities and requirements related to the implementation, administration and operation of the *Health Information Act*. Regardless of the size and structure of a custodian, fulfilling these responsibilities will require clear lines of responsibility and coordination within each organization.

Designating a person to be responsible for implementation and administration of the *Act* is not a requirement of the legislation but is part of a reasonable implementation strategy. The person designated will also be responsible for ensuring that the necessary *Health Information Act* related policies and procedures are established and followed. However, the custodian remains ultimately responsible for compliance with the *Act*.

In the case of the department, regional health authorities, provincial health boards, hospitals and nursing homes, as well as large multi-practitioner clinics, the task of designating a responsible person could be met by appointing an employee or other type of affiliate as a Health Information Coordinator. In the case of custodians such as small pharmacies and single physician offices, the licensed pharmacist, the physician or a member of their office staff could be designated as the responsible person.

If the custodian organization is large or decentralized, such as a regional health authority, it may choose to designate individuals responsible for the *Health Information Act* on a site by site or geographic basis, rather than having one person responsible for all the implementation tasks throughout the region or at all sites. Designated persons may be employees or agents of the custodian.

In some cases, the responsible affiliate or Health Information Coordinator may also be the person who is the FOIP Coordinator for the organization, under the *FOIP Act*. For other custodians, the health records manager may be designated as the responsible affiliate or Health Information Coordinator.

A single individual or agent may represent several custodians in a clinic or facility setting or in instances where custodians do not have the resources themselves to administer the *Act*. These arrangements should be formalized in some way (e.g. put in writing or added to a position description) to ensure that the scope of responsibility is clear.

BEST PRACTICE: *It may be more effective to have only one individual designated as the responsible affiliate or Health Information Coordinator, with support from site or area/program contacts, as necessary. If a single custodian is carrying out the duties of the responsible affiliate, he or she should have an individual designated as a backup coordinator or responsible affiliate in the event of his or her absence or inability to carry out these duties and responsibilities.*

Whomever is designated as having these responsibilities should be fully trained and have access to senior staff and decision-makers and the necessary resources and support.

Many of the implementation issues and tasks of the custodian related to implementation would become the responsibility of the designated individual. In addition to the implementation tasks set out in the ***Health Information Act* Implementation Checklist (and in #1 through #6 of this section)**, the responsibilities of this affiliate or Health Information Coordinator would include:

- implementing policies, guidelines and procedures to manage the custodian's compliance with the provisions of the *Act*;
- providing advice on the implementation and administration of the *Act* to the staff of the custodian;
- managing the process for tracking and responding to requests for access to or for correction or amendment of an individual's own health information;
- developing a plan for and ensuring that the business practices of the organization are reviewed and adjusted to comply with the privacy protection requirements of the *Act*;
- coordinating any negotiations, mediations, investigations, and audits with the Office of the Information and Privacy Commissioner; and
- ensuring consistency in the application of other acts and regulations which relate to the prohibition or restriction on disclosure of health information **(section 4)**.

- **Forecast volume of requests**

Prior to the *Act* coming into force, requests made to health authorities by individuals for access to their own health information were handled under the *FOIP Act*. Requests for access to an individual's own health information made to physicians were handled, for the most part, under practice guidelines based on a 1992 Supreme Court of Canada decision or under other rules or processes. When the *Act* is proclaimed in force, greater public awareness regarding the right of access may result in an increase in the number of requests.

- **Establish an appropriate implementation support team**

Depending upon the projected volume of requests, the amount and type of health information collected, used or disclosed, and the size and complexity of the organization, a custodian may wish to establish a team to support the responsible affiliate or Health Information Coordinator. In a large organization, such as a health authority, the team should include senior representatives from the parts of the organization that collect, use or disclose health information. It may also include a representative from information technology and systems, information or records management, legal services and human resources.

- **Identify and communicate with other "affiliated" custodians**

A regional health authority will have a level of responsibility for subsidiary health corporations, community health councils and perhaps hospitals and nursing homes funded to provide services in the region. It may be useful for the regional health authority to coordinate implementation activities with those other custodians who would also be affiliates of the regional health authority.

2. Establish a Communications Plan

The department is responsible for overall leadership and direction in communicating with the public about implementation of the *Act*.

In addition, each custodian should have an internal and external communication plan in place to provide key messages about the custodian's responsibilities and activities in implementing the *Act*, awareness activities for patients, clients and affiliates about how the operations will change to comply with the *Act* and any special messages and approaches to communicate with the media and special groups that interact with the custodian.

3. Establish a Training Plan and Conduct Awareness Training for the Custodian's Staff and Other Affiliates as Necessary.

A training plan in a medium to large organization should accommodate a variety of audiences and their requirements, including senior staff, members of the governing authority, staff who have daily contact with the public, site or facility Health Information Contacts or back–up Coordinators and specific staff groups such as information management and records management specialists, legal advisors, admitting office staff, etc.

Training and awareness in small offices or organizations will likely require that those in positions of responsibility and those who interact directly with individual patients will have to understand the rules in the *Act*, the implications of those rules and administrative requirements.

4. Assess the Status Quo

The following questions will point to the areas where a custodian's operations may be affected:

- Who are the affiliates of the custodian?
- What are the current practices related to collection, access, use, disclosure, disposition, data matching and security?
- What are the current practices for records management and archives?
- Are personal health numbers collected and used?
- What legal authority is in place to support existing collection, use and disclosure practices?
- What policies are in place for consent?
- What projects and activities (such as new information systems, data matching, etc.) will be affected by the *Act*?
- What contracts will be affected and how will they need to be changed to comply with the *Act*?

5. Develop Procedures for Tracking and Responding to Access Requests

See #5 of the detailed *Health Information Act* Implementation Checklist in Appendix 3 and also see Chapters 2 and 3 of this Publication.

6. Develop a Plan to Ensure Compliance with the privacy provisions of the Act.

See #6 of the detailed *Health Information Act* Implementation Checklist in Appendix 3 and also see Chapters 5, 6, 7, 8 and 11 of this Publication regarding privacy compliance.

9.5 HEALTH RECORDS MANAGEMENT OR INFORMATION MANAGEMENT AND INFORMATION TECHNOLOGY FUNCTIONS

The health records management and information management/technology function provide major support to the Health Information Coordinator or responsible affiliate for the effective administration of the *Act*. Each custodian should coordinate its efforts for managing, administering, controlling, providing security for and preserving all the records containing health information, including electronic data and information, in its custody or under its control, in order to meet the requirements of the *Act*.

The responsibilities of persons carrying out the health records and information management functions for a custodian include:

- establishing and maintaining an adequate level of information control to ensure that all records containing health information can be located and retrieved within the required time limits;
- establishing and maintaining information management systems for the custodian that comply with the privacy protection provisions of the *Act*;
- ensuring that health records retention and disposition schedules are established, approved in an authorized fashion, and applied for all health information in the custody or under the control of a custodian;
- ensuring that adequate safeguards and information security measures are in place for the protection of all health information;
- establishing procedures for authenticating the identity of individuals and of those persons to whom health information is disclosed;
- establishing procedures, in accordance with the regulations, for stripping, encoding or transforming individually identifying health information to create non-identifying information; and
- conducting privacy impact assessments for new systems, practices and data matching proposals.

Under **section 66**, a custodian may enter into an agreement with an "Information Manager" for the provision of various information technology services, as set out in that section. An Information Manager is a type of affiliate that provides information processing, storing, retrieving or disposing services, data transformation or information management or information technology functions.

Once an agreement with the Information Manager, is in place, the custodian may disclose health information to that affiliate and the information may then be used or disclosed for the purposes authorized in the agreement.

See section 5.3.2 in Chapter 5 of this Publication for further discussion on agreements with "Information Managers" and Chapter 11 for more guidance on Records and Information Management, Privacy and Security.

9.6 ESTABLISHING OR ADOPTING POLICIES AND PROCEDURES

Each custodian must establish or adopt policies and procedures that will facilitate the implementation of the *Act* and the regulations. Custodians must also provide the Minister or department, on request, with a copy of such policies and procedures **(section 63)**. Policies and procedures of custodians should cover all aspects of implementing and administering the *Act* but are particularly important in the area of ensuring the confidentiality of health information in their custody or under their control and the privacy of the individuals who are the subjects of that health information.

The policies and practices set out in this publication could form the basis of what is adopted by a custodian. Larger custodian organizations may already have substantial policies and procedures in place covering the collection, use, disclosure and protection of health information. These may only need to be reviewed and adjusted to comply with the legislation. Regulated health professionals may be guided by standards for health records or for the disclosure of health information published by their regulatory bodies.

For example, the College of Physicians and Surgeons of Alberta published a Bulletin on *Physicians' Office Medical Records* in February, 2000. Some sector-specific information on the management of health records has been referred to in **Chapter 11 of this Publication**.

Whenever a custodian makes a major change to its policies, the custodian must prepare a privacy impact assessment to ensure that the changes do not introduce any new risks to the privacy of health information **(section 64(1))**.

9.7 MANNER OF GIVING NOTICE

When the *Act* requires that a notice or any other document be given to a person (such as in **sections 9, 10, 12, 13, 14, 15**), **section 103** states that it must be given:

- by sending it to that person by prepaid mail to the last known address of that person;
- by serving it personally on the individual;
- by substitutional service if so authorized by the Commissioner (e.g. by double registered mail to the individual's last known address); or
- by means of a machine or device that electronically transmits a copy of a document, picture or other printed material by means of a telecommunications system (e.g. fax machine).

9.8 LIABILITIES, SANCTIONS AND PENALTIES

9.8.1 IMMUNITY FROM SUIT

If custodians act in good faith, the *Act* protects them from legal action that may be taken by an individual who feels that his or her health information was not collected, used or disclosed appropriately.

Section 105 states that no action lies and no proceeding may be brought against the Crown, a custodian or any person acting for or under the direction of a custodian, for damages resulting from anything done or not done by that person in good faith while carrying out duties and exercising powers under the *Act*. This includes any failure to do something where a person has discretionary authority to do something but does not do it.

The discretionary exceptions in **section 11** allow a custodian to exercise discretion in refusing an individual's access to all or part of his or her own health information. If an individual alleges that he or she suffered damage as a result of a custodian refusing access to the individual's own health information under one of the discretionary exceptions in the *Act*, the custodian would not face any legal consequences, if the refusal was done in good faith.

9.8.2 PROTECTION OF EMPLOYEE

Section 106(1) provides protection to "whistleblowers" who disclose confidential health information to the Commissioner under **section 83**. Under **section 83,** if an affiliate believes that a custodian or other person is collecting, using or disclosing health information in contravention of the *Act,* the affiliate may disclose that information to the Commissioner. The Commissioner must investigate and review the disclosure, and must not reveal the identity of the affiliate or the person to the custodian.

Section 106(1) protects an affiliate who makes such a disclosure to the Commissioner (blows the whistle) from any action that may negatively affect the affiliate's status, either by the custodian or by someone acting on behalf of the custodian **(section 106(1)(a))**.
A custodian or person acting on behalf of a custodian also cannot take any action against an affiliate who properly discloses information in accordance with the *Act* (e.g. in response to a request under **Part 2 (section 106(1)(b))**.

In order to take advantage of this protection under the *Act,* affiliates must have acted in good faith in disclosing information to the Commissioner.

A person who contravenes **section 106(1)** is guilty of an offence and is liable to a fine of not more than $10,000 **(section 106(2))**.

9.8.3 OFFENCES AND PENALTIES

Section 107 requires custodians and affiliates to cooperate with the Information and Privacy Commissioner or another person conducting the duties of the Commissioner under the *Act*.

No Custodian or Affiliate May Knowingly

- alter, falsify or conceal any record, or direct another person to do so, with the intent to evade a request for access to the record; or
- destroy any record subject to the *Act,* or direct another person to do so, with the intent to evade a request for access to the record.

No Person May Knowingly

- collect, use, disclose or create health information in contravention of the *Act;*
- gain or attempt to gain access to health information in contravention of the *Act;*
- make a false statement to, or mislead or attempt to mislead, the Commissioner or another person performing the duties, powers or functions of the Commissioner or other person under the *Act;*
- obstruct the Commissioner or another person in the performance of the duties, powers or functions of the Commissioner or other person under the *Act;*
- fail to comply with an order made by the Commissioner under **section 80** or by an adjudicator under **section 101**. These are the orders made by the Commissioner or an adjudicator on completing an inquiry, to dispose of the issues.

  - the order–making powers in those sections cover such matters as requiring a custodian to grant access to all or part of a record; requiring a custodian to refuse access to all or part of a record; confirming a decision of a custodian; requiring a person to stop collecting, using, disclosing or creating health information in contravention of the *Act;* or requiring a person to destroy health information collected or created in contravention of the *Act; and*

- use individually identifying health information to market any service for a commercial purpose or to solicit money unless the individual who is the subject of the health information has specifically consented to its use for that purpose.

No Researcher May Knowingly

- breach the terms and conditions of a research agreement entered into with a custodian under **section 54**.

No Information Manager May Knowingly

- breach the terms and conditions of an information management agreement entered into with a custodian under **section 66**.

No Person Intending to Use Non-Identifying Health Information for Data Matching May

- fail to comply with **section 32(2)**. This section requires the person to notify the Commissioner of an intention to use non-identifying health information for data matching purposes before performing the data matching.

An offence under this section may result either from a review requested by an applicant or other individual under **section 73**; an investigation under **section 84(a)**; or a disclosure to the Commissioner under **section 83** regarding a possible failure to comply with the rules in the *Act* about collecting, using or disclosing health information.

Fines

Any person who contravenes **section 107(6)** is guilty of an offence and is liable to a fine of not more than $50,000.

CHAPTER TEN

COMMISSIONER'S POWERS AND DUTIES

10.1 OVERVIEW

This Chapter will cover:

- how the Commissioner is appointed;
- the Commissioner's mandate and general powers;
- the Commissioner's monitoring role;
- the provision of advice by Commissioner;
- disclosure to the Commissioner;
- the Commissioner's powers to conduct investigations and inquiries;
- the Commissioner's power to compel production of records;
- the Commissioner's power to authorize a custodian to disregard requests;
- the inadmissibility of statements provided to the Commissioner;
- protection from liability;
- delegation of the Commissioner's powers;
- reviews and investigations;
- adjudicator process; and
- judicial review.

The Commissioner under the *Health Information Act* (the "*Act*") is the Information and Privacy Commissioner appointed under Part 3 of the *Freedom of Information and Protection of Privacy Act* (the "*FOIP Act*") **(section 1(1)(e))**. The Commissioner is responsible to monitor compliance by custodians with the provisions of the *Act* and to investigate complaints. The powers and duties of the Commissioner are set out in **sections 84 to 91** of the *Act*. The role of the Commissioner in conducting reviews and inquiries is set out in **sections 73 to 83 and sections 88 to 90** of the *Act*.

10.2 APPOINTMENT

The Commissioner is an Officer of the Legislature and is independent from government.

The Lieutenant Governor in Council, on the recommendation of the Legislative Assembly, appoints the Information and Privacy Commissioner to carry out the duties and functions set out in the *FOIP Act* **(section 43** of the *FOIP Act)*. The Information and Privacy Commissioner is also the Commissioner responsible to carry out the duties and functions set out in **Part 7** of the *Health Information Act*.

The Commissioner is appointed for a term of five years and is eligible for reappointment (**section 44** of the *FOIP Act*). The Commissioner may not be a Member of the Legislative Assembly (**section 43** of the *FOIP Act*). The Commissioner may resign, but may be removed or suspended from office only for cause or incapacity (**section 45** of the *FOIP Act*). This means that the Commissioner may not be removed by arbitrary or capricious action, but only for some reason affecting or concerning the ability or fitness of the Commissioner to perform the duties of the office.

The Lieutenant Governor in Council may designate a judge of the Court of Queen's Bench of Alberta to act as an adjudicator:

- when an investigation or review involves a custodian and the Commissioner was a

former member, employee or administrator of that custodian; or
- where, in the Commissioner's opinion, the Commissioner has a conflict of interest in a review or investigation **(section 96(1))**.

The adjudicator has the same powers as the Commissioner in disposing of an investigation or review **(section 97)**.

Oath of Office

Under **section 102(1)**, before beginning to perform his or her duties, the Commissioner must take an oath to faithfully and impartially perform the duties of Commissioner under the *Act* and not to disclose any information received by the Office except as provided for in the *Act*. This oath is administered by the Speaker or Clerk of the Legislative Assembly.

Any person employed or engaged by the Office of the Commissioner must, before beginning to perform their duties, also take a similar oath, as administered by the Commissioner **(section 102(2))**.

10.3 MANDATE AND GENERAL POWERS

Part 3 of the *FOIP Act* establishes the position of Information and Privacy Commissioner and a supporting office. The Office of the Information and Privacy Commissioner was established in 1995. The Information and Privacy Commissioner is the Commissioner responsible under the *Health Information Act* to ensure that custodians are complying with the letter and spirit of that *Act*.

The general powers of the Commissioner are listed in **section 84** of the *Act*.

The Commissioner has general responsibility for monitoring how the legislation is administered to ensure that its purposes are achieved. Specifically, he or she may:

- conduct investigations to ensure compliance with any provision of the *Act* or compliance with rules relating to the destruction of records in accordance with rules set out the *Act* or any other enactment of Alberta **(section 84)(a))**;
- make an order regarding duties imposed by the *Act* such as granting or refusing access to a record or reconsidering a decision, administrative matters such as extensions of time and payment of fees, and the correction, collection, use, disclosure, creation or destruction of health information as described in **section 80(2)and (3)**. Such an order can be made whether or not a review is requested **(section 84(b))**;
- inform the public about the *Act* **(section 84(c))**;
- receive comments from the public about the administration of the *Act* **(section 84(d))**;
- engage in or commission a study into anything affecting the achievement of the purposes of the *Act* **(section 84(e))**;
- comment on the implications for access to health information or for protection of health information of privacy impact assessments submitted to the Commissioner **(section 84(f))**;
- comment on the implications for protection of health information of using or disclosing health information for data matching **(section 84(g))**;
- bring to the attention of a custodian any failure by a custodian to assist applicants under **section 10 (section 84(i))**; and

- give advice and recommendations of general application to a custodian regarding the rights and obligations of custodians (**section 84(h)**). The Commissioner may use this power to suggest improvement in the way a custodian deals with requests. This power will likely only be used when there is evidence of poor administration, such as inadequate training or failure to locate records; where there is wanton disregard for the provisions of the *Act*; or where there are systemic problems, such as regular delays, improper interpretation of exceptions or complaints about breaches of protection for health information.

Further, without limiting the general powers in **section 84**, the Commissioner may investigate and attempt to resolve complaints that:

- a duty imposed by **section 10** (duty to assist applicants) has not been performed (**section 85(a)**);
- an extension of time for responding to a request is not in accordance with **section 15** (time extensions) (**section 85(b)**);
- a fee charged under the *Act* is inappropriate (**section 85)(c)**);
- a correction of health information requested under **section 13** has been refused without justification (**section 85(d)**); or
- health information has been collected, used, disclosed or created by a custodian in contravention of the *Act* (**section 85(e)**).

The Commissioner has sole jurisdiction to investigate matters of access to health information and the protection of health information that are governed by the *Act*. The *Act* specifically prohibits the Ombudsman from investigating any matter within the jurisdiction of the Commissioner unless the Commissioner agrees (**section 94**).

An order issued by the Commissioner is final (**section 81**). However, the Courts have inherent and constitutional jurisdiction to review and determine whether the Commissioner has acted within the authority given to the Office under the *Act*. This is known as the common law principle of *judicial review*.

As an independent Officer of the Legislature, the Commissioner reports annually to the Speaker of the Legislative Assembly describing the work of the Commissioner's Office and such other matters relating to the protection of health information that the Commissioner considers appropriate (**section 95(1)**).

Further information, including copies of brochures, news releases, orders, investigation reports and annual reports, is available at the web site of the Office of the Information and Privacy Commissioner, at **http://www.oipc.ab.ca**

10.4 MONITORING ROLE

A number, but not all, of the powers of the Commissioner are discussed below.

The Commissioner may investigate the administration of the *Act* by custodians. The Commissioner may also audit the practices of custodians in the areas of access to health information and protection of health information.

In the area of access to health information, the Commissioner may, for example:

- examine a custodian's compliance with the time limits imposed by the *Act*;
- investigate allegations that records are being destroyed to avoid producing them in response to a request under the *Act*; or
- review the decision of the custodian to refuse a request for a fee waiver, if requested to do so by the applicant (**sections 67((4) and (5)**).

In the area of protection of privacy of health information, the Commissioner may, for example:

- review the collection of health information by a custodian to ensure it has the legal authority to collect the information (**section 18**) or is complying with the rules for indirect collection (**section 22(2)**);
- review the records disposition practices of a custodian to ensure that it is retaining health information as required by the *Act*;
- review privacy impact assessments as required under **sections 46, 50, 70, 71 and 72** of the *Act*;
- audit a custodian's fair information practices within a program or health information system to ensure compliance with the *Act*; or
- investigate the application of new information technology to ensure that protection of health information is being adequately addressed.

The Commissioner may also examine and comment on legislation and program activities in terms of any implications for access to health information and the protection of health information.

Examples of such legislation and program activities include:

- the amendment of a statute or by-law to include provisions for introducing personal identifiers, or to allow release of health information. The Commissioner could examine a custodian's reasons for including such amendments and comment on their relationship to the provisions and intent of the *Health Information Act*; and
- the enhancement of service delivery through implementation of a "smart card" using health information for a variety of purposes.

The Commissioner might advise the custodian as to the need for a Privacy Impact Assessment for the project. By commenting on and informing the public about the implications of legislative and other proposals of custodians the Commissioner can help them to comply with the spirit of open government and access and protection of health information rights and to be accountable for their actions.

The Commissioner may review automated information systems to ensure that they comply with the *Act*.

The Commissioner also has the mandate to conduct or commission research into any issue affecting the way in which the purposes of the *Act* are being achieved.

The Commissioner's role in dealing with reviews and complaints from persons not satisfied with the handling of a request for access to or correction of health information is discussed in section 10.13 of this Chapter.

10.5 PROVISION OF ADVICE

The Commissioner may provide a custodian with advice and recommendations on matters respecting the rights or obligations of custodians under the *Act* **(section 84(h))**. Further, a custodian may ask the Commissioner to give advice and recommendations on any matter respecting any rights or duties under the *Act* **(section 86(1))**.

Some examples of advice that may be given under **section 86** have been provided earlier in this chapter.

The Commissioner may include advice or recommendations to a custodian in an order or an investigation report **(section 86(2))**.

A custodian might seek advice from the Commissioner on general procedures or matters of interpretation relating to an access request pursuant to **Part 2** of the *Act* **(Individual's Right to access Individual's Health Information)**, or on how to appropriately apply the health information protection provisions of **Parts 3 to 6** of the *Act* **(Collection, Use and Disclosure of Health Information and Duties and Powers of Custodians Relating to Health Information)**. The advice will normally be sought through a letter from a custodian to the Commissioner. Advice given in response to a request from a custodian must be of a general nature and not anticipate or relate to a specific case. It can include recommendations on the administration and application of the *Act* generally or more particularly to a certain custodian.

Section 86(2) provides that the Commissioner may respond to a custodian in writing with advice and recommendations that:

- state the material facts either expressly or by incorporating facts stated by the custodian;
- are based on these facts; and
- are based on any other considerations that the Commissioner considers appropriate.

10.6 DISCLOSURE TO THE COMMISSIONER

The Commissioner must investigate and review any disclosure made to him or her by an affiliate of a custodian of any information that an affiliate is required to keep confidential and that the affiliate, acting in good faith, believes is being collected, used or disclosed in violation of the *Act* **(sections 83(1) and (2))**.

The Commissioner must not disclose the identity of the affiliate to any person without the affiliate's consent **(section 83(3))**.

In carrying out an investigation and review under this provision, the Commissioner has the powers of mediation, investigation, inquiry and order making described in **section 83(5)**, as well as the protection provided by **section 83(4)**.

10.7 POWERS TO CONDUCT INVESTIGATIONS OR INQUIRIES

The Commissioner has all the powers, privileges and immunities of a commissioner under the *Public Inquiries Act* **(section 88(1))** when conducting an investigation under **section 84(a)** or an inquiry under **section 77**, or when giving advice and recommendations under **section**

86 of the *Act*. These powers, privileges and immunities include the power to compel witnesses to attend and answer questions at an inquiry, to compel records to be produced, to hold a person in contempt and to obtain assistance from law enforcement officers.

10.8 ACCESS TO INFORMATION

The Commissioner may require any record to be produced and may examine any information in a record, whether or not the record is subject to the provisions of the *Act* **(section 88(2))**.

A custodian must produce any record or copy of a record requested by the Commissioner under **section 88(1)** or **(2)** within 10 days **(section 88(3))**. This must be done regardless of any other enactment of Alberta but not if a federal enactment, such as the *Young Offenders Act* (Canada), prohibits disclosure **(see IPC Order 96-015)**. Records must be produced despite any privilege of the law of evidence that might otherwise apply **(section 88(3))**. This requirement applies to records that the custodian believes to be excluded from the coverage of the *Act* **(see IPC Practice Note No. 4, Section 4 – Exclusions from the Act)**.

If a custodian is required to produce a record and it is not practicable to make a copy of it, the custodian may request that the Commissioner examine the original at the site of the custodian **(section 88(4))**.

The Commissioner must return all records or copies of records to the custodian after completing a review or investigating a complaint **(section 88(5))**.

10.9 AUTHORIZING CUSTODIANS TO DISREGARD REQUESTS

A custodian may, under **section 87** of the *Act*, request the Commissioner to authorize the custodian to disregard requests from an applicant. This applies to both requests for access to information and requests for correction or amendment of health information. A custodian must present facts in support of its request. The Commissioner then makes a decision. A custodian may be allowed to disregard a request if it is:

- repetitious or systematic in nature, and processing the request would unreasonably interfere with the operations of the custodian, or amount to an abuse of the right to make requests; or
- frivolous or vexatious.

See section 2.4.9 of Chapter 2 of this Publication for more detail on Dealing with Repetitious or Systematic Requests, including explanations for "repetitious", "systematic", "unreasonable interference with operations of custodian", "abuse of the right of access" and "frivolous or vexatious".

Asking for authorization to disregard requests should be rare. Custodians should ensure that they have fully discharged their duty to assist applicants in a full and forthright manner and have a strong case before seeking permission from the Commissioner to disregard requests from one or more applicants.

10.10 STATEMENTS PROVIDED TO THE COMMISSIONER

A statement made or an answer given by a person during an investigation or inquiry by the Commissioner is inadmissible in evidence in court or in any other proceeding, except:

- in a prosecution for perjury in respect of sworn testimony;
- in a prosecution for an offence under the *Act*; or
- in an application for judicial review or an appeal from a decision of that review **(section 89(1))**.

These conditions also apply to evidence from proceedings conducted before the Commissioner **(section 89(2))**.

Anything said, any information supplied or any record produced by a person during an investigation or inquiry by the Commissioner is privileged. The rules that apply are those for a proceeding before a court **(section 90)**.

Section 91 of the *Act* places restrictions on the disclosure of information by the Commissioner and the staff of the Office of the Information and Privacy Commissioner. They must not disclose any information they obtain in the performance of their duties, with the following exceptions:

- disclosure of information that is necessary for the conduct of an investigation under the *Act* or to establish the grounds for findings and recommendations made under the *Act* **(section 91(2))**;
- disclosure to the Minister of Justice and Attorney General information relating to the commission of an offence against an enactment of Alberta or Canada, if the Commissioner believes there is evidence of an offence **(section 91(4))**; and
- disclosure of information in the course of a prosecution for perjury or for an offence under the *Act*, or in an application for judicial review or an appeal arising from that application **(section 91(5))**.

During the conduct of an investigation or inquiry and when writing a report, the Commissioner and the staff of the Office of the Information and Privacy Commissioner must not disclose any information a custodian would be required or authorized to refuse to disclose. They must also ensure that they do not disclose the fact that information exists where, in the refusal to provide access, the custodian did not indicate whether the information exists **(section 91(3))**.

10.11 PROTECTION FROM LIABILITY

The Commissioner and his or her staff are not liable for anything they do in good faith in the exercise of their duties, powers or functions under **Part 7** of the *Act* **(The Commissioner) (section 92)**.

As long as the Commissioner and his or her staff act honestly and with the intention of complying with the *Act*, no action can be brought against them.

10.12 DELEGATION OF THE COMMISSIONER'S POWERS

Section 93(1) provides that the Commissioner may delegate, in writing, to any other person any duty, power or function of the Commissioner under the *Act*. The only exception to this provision is that the Commissioner cannot delegate the power to delegate.

This allows the Commissioner to delegate powers to the Assistant Commissioner, to delegate the power to examine law enforcement information and Cabinet documents, to authorize custodians to disregard requests and to hold inquiries and issue orders on completion of those inquiries.

10.13 REVIEWS AND INVESTIGATIONS

Reviews

Section 73 of the *Act* provides individuals who have made a request for access to or correction to or amendment of their own health information under **Part 2** of the *Act* with the right to ask the Commissioner to review any decision, act or failure to act by a custodian **(section 73(1))**.

An individual who believes that his or her health information has been collected, used, or disclosed in contravention of the *Act* may also ask the Commissioner to review the matter **(section 73(2))**.

Section 73(3) enables a custodian to ask the Commissioner to review the refusal of another custodian to disclose health information pursuant to **section 47(2).**

The right to an impartial review of decisions or actions of a custodian is fundamental to guaranteeing access to health information and protection of health information. The review mechanism ensures that these rights are interpreted consistently among custodians and the purposes of the *Act* are achieved. The orders, which summarize the reviews, issues, reasons, and findings of the Commissioner, also provide guidance to custodians regarding the proper interpretation of the *Act*.

A review by the Commissioner of the decision of a custodian is intended to be an avenue of last resort. In most cases, an individual will be satisfied that the custodian has acted responsibly and any outstanding issues can be settled between the custodian and the person concerned. Even in cases where the person asks the Commissioner to review a decision, issues can often be settled through mediation and an inquiry may not be necessary.

Certain matters that may be the subject of a request for review can also be grounds for a complaint to the Commissioner under **section 85** of the *Act*.

These are matters relating to:

- the custodian's duty to assist the applicant as required in **section 10**;
- a decision to extend the time limit for responding to a request is not in accordance with **section 15**;
- a fee charged under **section 67**;
- a refusal to make a correction to health information as requested under **section 13(1)**; and

- the collection, use, disclosure or creation of health information in contravention of the *Act*.

Requesting a Review

Section 74 of the *Act* sets out the process for requesting a review. A **Flowchart of the Review Process** is provided in **Figure 10**. The Office of the Information and Privacy Commissioner provides a **Request for Review Form** for this purpose.

A copy of the form is included in Appendix 1 of this Publication.

Applications for a review can be made on this form or by letter, but in all cases must be in writing **(section 74(1))**. **Section 104** establishes classes of individuals who may act for deceased persons, incompetent persons, minors, formal patients under the *Mental Health Act* and any other individuals in exercising this right under the *Act*.

A person must deliver a request for a review to the Commissioner within 60 days of receiving notification of a custodian's decision or a longer time when allowed by the Commissioner **(section 74(2))**.

Failure by a custodian to respond in time to a request for access to a record is treated as a decision to refuse access (deemed refusal) **(section 74(3))**.

Preparation for a Review

A custodian must be able to show that it has properly fulfilled its duties under the *Act*. It should document the reasons for each decision relating to the withholding of records or parts of records and should ensure that the circumstances surrounding the request support each action it takes.

To reduce the need for review of decisions, custodians should provide applicants with clear explanations of their decisions, the provision(s) of the *Act* that apply and the reasons why they are applicable in the particular instance. These explanations provide a basis for discussion of the decision and may help the custodian and the person to settle any outstanding issues without recourse to the Office of the Information and Privacy Commissioner. This point is discussed in **IPC Practice Note No. 2, 'Informing the Applicant of Grounds for Refusal'.**

Review Process

The Office of the Information and Privacy Commissioner has developed procedures for conducting reviews and public inquiries and these are available from that office.

IPC Practice Note No. 5, 'Preparing Records and Submissions for Inquiries' should also be carefully read. The *Act* has enabling provisions and some requirements governing the review process.

Upon receiving a request for review, the Commissioner must provide a copy of the request to the custodian and to any other person the Commissioner believes is affected by the request **(section 75(1)(a))**.

The Commissioner must also provide a summary of review procedures and an anticipated date for a decision regarding the review to the person who asked for the review, to the custodian and to any other person affected by the request **(section 75(1)(b))**.

The Commissioner may sever any information in the request that he/she considers appropriate before providing copies as stated above **(section 75(2))**. This is necessary because applicants may include health information as a part of their request for review, and it may not be appropriate to disclose this to the custodian or to other persons.

The staff of the Office of the Information and Privacy Commissioner, the custodian and the applicant will jointly review the request to determine whether the concerns raised in it can be addressed through mediation.

The Commissioner will also ask the custodian to submit copies of the following documentation, where applicable:

- the request for access to information under **Part 2** of the *Act*;
- notice of the custodian's decision;
- any correspondence related to the request, issue or decision;
- an index of the relevant records and exceptions relied upon;
- severed and unsevered copies of the records; and, where applicable,
- the custodian's policies and procedures related to its management and protection of health information under **Parts 3 to 6** of the *Act* **(Collection, Use and Disclosure of Health Information and Duties and Powers of Custodians Relating to Health Information)**.

The custodian may initially be more familiar with the issues involved than the Office of the Information and Privacy Commissioner. If the custodian has any information concerning affected persons who should be notified of the review, it should inform the Office as soon as possible.

The custodian should also make known any relevant issues, considerations or factors that affected the making of the particular decision. The Commissioner will have a better understanding of the custodian's position if it can demonstrate that it made every effort to meet an individual's needs and to resolve outstanding issues.

Mediation

Section 76 provides that the Commissioner may authorize a mediator to investigate and try to settle any matter that is the subject of a request for a review. In most cases, the Commissioner will instruct a Portfolio or Compliance Officer to proceed in this way. The mediator does not impose a settlement. Rather, mediation is intended to help the custodian and the person requesting a review to arrive at a settlement before a formal inquiry is initiated.

Inquiry

If a mediator is not appointed or the matter is not resolved with the help of a mediator, the Commissioner normally conducts an inquiry **(section 77(1))**.

In the course of the inquiry, the Commissioner will decide all questions of law and fact.

The Commissioner's powers in conducting inquiries are provided in **sections 77 and 88** of the *Act*.

The Commissioner has broad discretion to determine how an inquiry will be conducted. It may be conducted in private **(section 77(2))** and the Commissioner may decide whether representations are to be made orally or in writing **(section 77(4))**.

The person who asked for the review, representatives of the custodian concerned and any person given a copy of the request for review are entitled to make representations to the Commissioner during the inquiry **(section 77(3))**. These persons may choose to be represented by counsel or an agent **(section 77(5))**.

No party has a right to be present during another party's representations, to have access to or to comment on representations made by another person during the inquiry process **(section 77(3))**.

In the case of a refusal of access, the Commissioner has the right and duty to view all records that have been withheld from disclosure in whole or in part. This right pertains regardless of the exception that the custodian has used or the fact that the custodian believes the records are excluded from the scope of the *Act*.

The Commissioner may require the records to be produced within 10 days **(section 88(3))**. The Commissioner must return such records to the custodian upon completion of the review **(section 88(5))**.

The custodian may require the Commissioner to examine an original record at the site at which it is being held, if it is not practical to make a copy **(section 88(4))**. This could occur, for example, when a record is too fragile to copy or the copying process would damage the record. Custodians should avoid, as much as possible, requiring on-site examination of records since it will place an additional administrative burden on their own and the Commissioner's operations.

The Commissioner may compel witnesses to attend an inquiry and to answer questions. The Commissioner has all the powers of a Commissioner provided under the *Public Inquiries Act* **(section 88(1))**. These powers include the power to hold a person in contempt and to obtain the assistance of law enforcement officers to compel attendance at an inquiry or to compel records to be produced.

Refusal to Conduct Inquiry

Over time, issues raised in requests for review may replicate issues already dealt with by the Commissioner. If the Commissioner believes that the subject matter of a request has already been dealt with in an order or an investigation report, the Commissioner may refuse to conduct an inquiry **(section 78)**.

Time Limits for Review

Normally, the Commissioner's inquiry must be completed within 90 days after receipt of the request for review **(section 77(6))**. This time limit encompasses all elements of the review process, including mediation and any formal inquiry.

However, the Commissioner may notify all parties to a review that he or she is extending the period for the review and establish a date for the completion of the review **(section 76(6))**. The intent of the *Act* is to ensure that an independent review of decisions can take place, so even if the process is not completed within the extended time limit, the Commissioner has the power to complete the inquiry **(see IPC Order 99-011)**.

Burden of Proof

Section 79 establishes where the burden of proof lies in various situations relating to access to records. Normally, the burden of proof rests with the custodian refusing access to all or part of a record **(section 79)**.

This means that under normal circumstances the custodian must prove, on the balance of probabilities, that particular information may be excepted from release under the *Act* or excluded from its scope.

Careful documentation of the reasons for refusing the request will form the central arguments that will meet the burden of proof.

A custodian also has the burden of proof in cases where an applicant has requested a review of fees charged **(see IPC Order 99-014)**. This is because the custodian has all the information about the assessment and calculation of fees.

Commissioner's Orders

Upon completion of an inquiry, **section 80(1)** of the *Act* requires the Commissioner to make an order. If the inquiry concerns a refusal to grant access to all or part of a record, the Commissioner may order one of the following under **section 80(2)**:

- require the custodian to give access to all or part of the record;
- confirm the decision of the custodian or require the custodian to reconsider a decision to refuse access; or
- require the custodian to refuse access to part or all of the record requested.

When the Commissioner finds that a refusal to grant access is in compliance with the *Act*, and the custodian has properly exercised his or her discretion, the Commissioner may only confirm the decision of the custodian or request that the custodian reconsider the decision based on its exercise of discretion.

The Commissioner can only require the custodian to reconsider a decision to refuse access, not a decision to grant access **(see IPC Order 98-001)**.

If the inquiry concerns any other matter, such as the matters discussed in **section 85**, the Commissioner may make an order requiring compliance with the provisions of the *Act*. Under **section 80(3)**, the Commissioner may:

- require a duty imposed by the *Act* or regulations to be performed;
- confirm or reduce the extension of a time limit under section 15;
- confirm or reduce a fee required to be paid or to order a refund, including where a time limit is not met;
- confirm a decision not to correct or amend health information or specify how health information is to be corrected or amended;
- require a person to stop collecting, using, disclosing or creating health information in contravention of the *Act*; or
- require a person to destroy health information collected or created in contravention of the *Act*.

Section 85(4) provides that the Commissioner may attach any terms or conditions to an order. A copy of the order is given to the person who asked for the review, the custodian concerned, any person given a copy of the request for review, and the Minister responsible for the administration of the *Act* **(section 85(5))**.

A custodian that has received an order from the Commissioner must comply with the order no earlier than 45 days after the order, and no later than 50 days after the order **(section 82(1) and (2))**. This is to allow the parties time to apply for judicial review.

If an application for judicial review is made, the Commissioner's order is stayed until the Court has dealt with the application **(section 82(4))**.

There is no appeal from an order made by the Commissioner (**section 81**) except a limited appeal through judicial review (**see section 10.15 of this Chapter**).

It is an offence to fail to comply with an order made by the Commissioner under **section 80 (section 107(2)(e))**. The Commissioner may choose to file a copy of an order with the clerk of the Court of Queen's Bench and, after filing, the order is enforceable as a judgment or order of that Court (**section 80(6)**).

Investigations

Section 84 of the *Act* enables the Commissioner to monitor compliance with the *Act* and carry out investigations into how the *Act* is being administered to ensure that its purposes are achieved. **Section 85,** without limiting these more general powers, enables the Commissioner to investigate and attempt to resolve complaints that:

- a duty imposed by **section 10** (duty to assist has not been performed);
- an extension of time for responding to a request is not in accordance with **section 15**;
- a fee charged under the *Act* is not appropriate;
- a correction or amendment of health information requested under **section 13** has been refused without justification; or
- health information has been collected, used, disclosed or created by a custodian in contravention of the *Act*.

The main difference between an investigation and a review is that an investigation may not be a result of a request for access to health information under **Part 2** of the *Act*. A complaint that does not arise from an access request is most likely to arise in cases involving allegations of improper collection, use, disclosure or creation of health information.

When an investigation is held into an alleged breach of protection of health information (**section 85(e)**), a Portfolio or Compliance Officer from the Office of the Information and Privacy Commissioner is assigned to investigate the matter. When the investigation is complete, an investigation report is prepared and sent to both parties. It includes the Portfolio or Compliance Officer's findings and recommendations. The complainant is asked whether the report satisfies his or her concerns and the custodian is asked to inform the Portfolio or Compliance Officer how it will comply with the recommendations.

If the complainant is satisfied with the report's finding and recommendations, and the custodian accepts the recommendations, the Portfolio or Compliance Officer forwards the report to the Commissioner and advises that the complaint has been resolved.

If the complainant is not satisfied with the findings and recommendations, he or she can request that the matter proceed to inquiry in accordance with **section 73(2)**.

In this case, the report of the Portfolio or Compliance Officer is not forwarded to the Commissioner and is not publicly released. Evidence collected during the investigation is not normally forwarded to the Commissioner for the inquiry.

For further details on the process of dealing with the investigation of complaints see **IPC Practice Note No. 7, 'Privacy Complaints – Investigations and Inquiries'**.

Custodians are always informed by the Office of the Information and Privacy

Commissioner as to whether an issue is subject to a review **(section 74)** or an investigation **(section 84(a))**. The preparation and response to an investigation will be very similar to those outlined for the review process described above **(see IPC Practice Note No. 3, 'Complaints about Public Bodies –Reviews versus Investigations')**.

Time Limits on Complaints

When an investigation arises from a *Health Information Act* request, the applicant must deliver the complaint to the Commissioner within 60 days of receiving notification of the custodian's decision **(section 74(2)(a))**.

A longer time may be allowed by the Commissioner **(section 74(2)(b))**. When allowing a delay, the Commissioner will consider all relevant circumstances.

The *Act* does not specify a time limit for filing complaints about a breach of health information privacy, since these do not, for the most part, arise from a request for access to health information under **Part 2** of the *Act*. They tend to stem from a complainant's belief that there has been improper collection, use, disclosure or creation of health information.

Privacy Investigations and Audits

The Commissioner can take an active role in investigating compliance with **Parts 3 to 6 (Collection, Use and Disclosure of Health Information and Powers and Duties of Custodians Relating to Health Information)**. An investigation can be undertaken as a result of a complaint that health information is not being collected, used, disclosed or created in accordance with the provisions of the *Act*.

As well, the Commissioner may decide to conduct an audit of the management and protection of the privacy of health information collected, used or disclosed in a program of a custodian. The Commissioner's practice is to make all Investigation Reports and Health Information Privacy Audit Reports public.

Refer to Chapter 11 of this Publication for a checklist to help custodians determine whether they currently comply with the requirements of Parts 3 to 6 of the *Act*.

The Checklist also serves as a guide for remedial measures that may be necessary to adequately protect the health information in the custody or under their control of custodians.

10.14 ADJUDICATOR PROCESS

Section 96 provides for the appointment of an adjudicator. This occurs in situations when the Commissioner is not in a position to conduct an investigation or review because there would be an apprehension of bias. This can occur when the Commissioner has been a member, employee or administrator of a custodian in a capacity directly related to the matter under investigation or review, or when the matter relates to the Office of the Information and Privacy Commissioner or any other Office of the Legislature of which he or she is the head.

The Commissioner makes the determination that he or she has a conflict of interest **(section 96(1))**.

An adjudicator cannot review an order of the Commissioner **(section 96(2))**.

An applicant or custodian seeking a review under **section 73** of the *Act* when these circumstances exist may request that an adjudicator be appointed to conduct the review **(section 98).**

The request must be in writing to the Minister responsible for the *Act* **(section 99(1))**. The request must be delivered to the Minister within 60 days of the person receiving notice of the decision to be reviewed **(section 99(2)(a))**. The adjudicator may decide that a longer period should be allowed **(section 99(2)(b))**.

Upon receipt of the request, the Minister must facilitate the appointment of an adjudicator, give the request to him or her and also give a copy to the Commissioner and to any other person who is affected by the request **(section 100(a) and (b))**. The Minister must also provide a summary of the review procedures to the person that asked for the review and to the Commissioner and to any other person who is affected by the request **(section 100(c)).**

The Minister will confirm with the Commissioner that a conflict exists and will verify that the request is valid. Documentation needed to allow the Minister and Cabinet to review the request will be compiled. Alberta Justice is responsible for requesting the Chief Justice of Alberta to nominate a judge of the Court of Queen's Bench to act as adjudicator.

A submission is made to Cabinet to authorize the Lieutenant Governor in Council to designate the judge to act as an adjudicator. The Minister must provide a copy of the applicant's request for review, together with a summary of the review procedures that will govern the process, to the adjudicator, the Commissioner and any other person affected by the request.
This is currently the process followed for the appointment of an adjudicator under the *FOIP Act.*

An adjudicator has the same powers and duties as the Commissioner and can dispose of a matter in the same way **(sections 97 and 101(1) and (2))**. A copy of the adjudicator's order must be given to the Commissioner **(section 101(3))**. An order made by an adjudicator is final **(section 101(6))**. The duty to comply with an order and the time periods for applying for judicial review in **section 82** apply to an order of an adjudicator **(section 101(5))**.

The Government of Alberta may pay the adjudicator and the adjudicator's expenses for retaining persons to assist the adjudicator **(section 96(4))**.

10.15 JUDICIAL REVIEW

The Commissioner has exclusive jurisdiction to conduct a review and investigate complaints against a custodian under the *Act*. Courts do not have the power to issue orders under the *Act*.

However, a person may apply to the Court of Queen's Bench of Alberta to exercise its inherent jurisdiction to review any action or failure to act on the part of the Commissioner **(or an adjudicator where one has been appointed)**. It may also review the decisions of the Commissioner for an error of law on the face of the record, jurisdictional error or breach of natural justice (fairness).

Application for judicial review of a decision of the Commissioner must be made not later than 45 days after the party applying for judicial review is given a copy of the decision **(section 82(3))** unless the court extends this period **(section 82(5))**.

When an application is made for judicial review, the Commissioner's order is stayed **(section 82(4))**.

The Court has the power to compel the Commissioner to do something or to refrain from doing something and the power to send a matter back to the Commissioner for reconsideration.

A judicial review is not an appeal of the Commissioner's decision. The Court cannot substitute its own decision for that of the Commissioner. The Commissioner is the final arbiter of questions of fact but is always subject to the overriding jurisdiction of the Court to ensure that the Commissioner acts within his or her authority.

Information and Privacy Commissioner Review Process

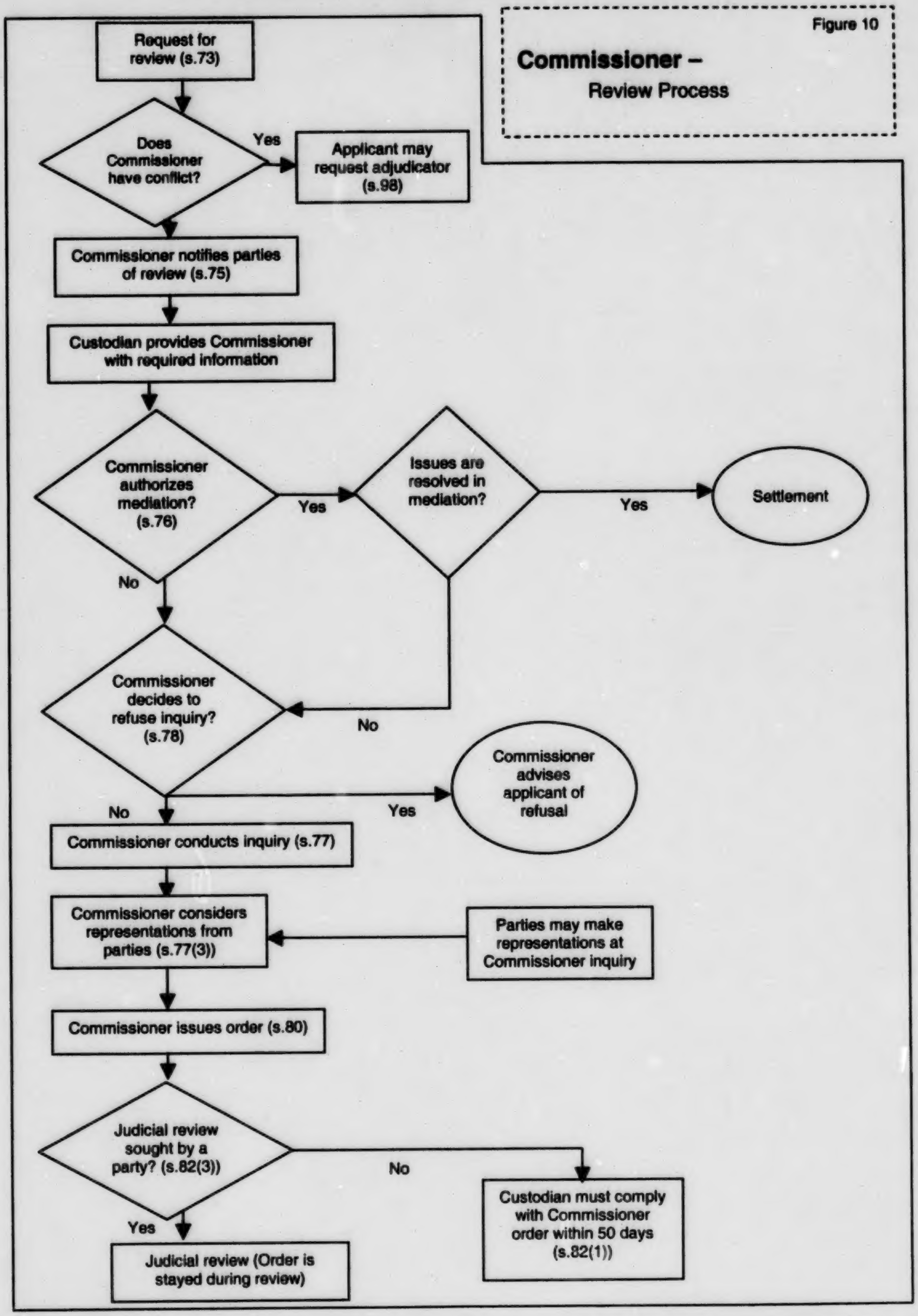


Figure 10

Commissioner –
Review Process

Request for review (s.73)
Does Commissioner have conflict?
Yes
Applicant may request adjudicator (s.98)
Commissioner notifies parties of review (s.75)
Custodian provides Commissioner with required information
Commissioner authorizes mediation? (s.76)
Yes
Issues are resolved in mediation?
Yes
Settlement
No
Commissioner decides to refuse inquiry? (s.78)
No
No
Yes
Commissioner advises applicant of refusal
Commissioner conducts inquiry (s.77)
Commissioner considers representations from parties (s.77(3))
Parties may make representations at Commissioner inquiry
Commissioner issues order (s.80)
Judicial review sought by a party? (s.82(3))
No
Custodian must comply with Commissioner order within 50 days (s.82(1))
Yes
Judicial review (Order is stayed during review)

CHAPTER ELEVEN

RECORDS AND INFORMATION MANAGEMENT, PRIVACY AND SECURITY

11.1 OVERVIEW

This Chapter will cover:

- the purposes for records and information management;
- the powers of the Information and Privacy Commissioner to conduct investigations to ensure compliance with rules relating to the destruction of health records;
- records issues relating to access requests;
- records and information management principles;
- records and information management policy components;
- how to review compliance with **Parts 3 to 6** of the *Act* **(Collection, Use and Disclosure of Health Information and Powers and Duties of Custodians Relating to Health Information)**;
- how to review forms used in the collection of health information to ensure they meet the collection and notification requirements of the *Act*;
- how to conduct an assessment of threats and risks to the security of health information; and
- how to develop a health information security policy that supports the duty to protect the privacy of individuals and the confidentiality of their health information.

11.2 RECORDS AND INFORMATION MANAGEMENT

To meet their obligations under the *Health Information Act*, custodians need to have in place effective records and information management practices. This Chapter is intended to help custodians understand how these practices assist in the effective administration of the *Act*.

Records and information management is generally carried out to:

- support policy formation and managerial decision-making;
- improve client services and support better performance of business activities;
- support consistency, continuity and productivity in operations, administration and management;
- protect the interests of the organization and the rights of clients, the public and employees;
- provide protection and evidentiary support in litigation;
- facilitate research and development activities; and
- enable the organization to meet legislative and regulatory requirements.

The department, as well as its agencies, boards and commissions under Schedule 1 of the FOIP Regulation are subject to the Records Management Regulation (AR 57/95) and must adhere to the policies and guidelines established under this Regulation.

Other custodians must adhere to the policies or guidelines regarding retention and disposition of records established under an enactment. For example, **section 15 of the Operation of Approved Hospitals Regulation** under the *Hospitals Act* or

sections 15 16, 17 and 18 of the Pharmaceutical Profession Regulation under the *Pharmaceutical Profession Act*, establish retention and disposition practices for approved hospitals and pharmacists, respectively. The College of Physicians and Surgeons of Alberta published a bulletin on "Physician's Office Medical Records" which included guidelines on retention and disposition of medical records. This was done pursuant to the authority of the College to regulate the practice of medicine under the *Medical Profession Act*.

For the department and other custodians, **section 3(c)** of the *Health Information Act* authorizes the transfer, storage or destruction of health records if it is done in accordance with an enactment of Alberta or Canada. The scheduling and disposition of health records must take into account the importance of an authorization process that ensures the custodian can meet its financial, legal and ethical obligations, including its obligations under the *Health Information Act*.

Custodians are required, under **section 60(2)**, to maintain administrative, technical and physical safeguards that include appropriate measures for the proper disposal of records to prevent any reasonably anticipated unauthorized use or disclosure of the health information or unauthorized access to the health information following its disposal.

11.2.1 POWERS OF THE COMMISSIONER

Section 84(a) authorizes the Information and Privacy Commissioner to monitor the general administration of the Act to ensure that its purposes are achieved. This includes conducting investigations to ensure compliance with rules relating to the destruction of health records set out in any other enactment of Alberta.

Custodians should expect their records and information management practices to be under scrutiny during reviews, investigations and health information privacy audits conducted by the Office of the Information and Privacy Commissioner. This is especially the case when an applicant requests a review of the adequacy of a search for information or records.

11.2.2 RECORDS ISSUES RELATING TO ACCESS REQUESTS

The right of access to an individual's own health information in health records, which is provided in **Part 2** of the *Act*, is intended to make custodians more open and accountable to individuals regarding their own health information. Inadequate record keeping can contribute to poor accountability to clients and patients.

In the case of right of access requests, a custodian may find that poor records management can cause it to violate the Act.

This may lead to:

- challenges to the credibility and reputation of the custodian;
- costly use of resources to defend past actions rather than the use of resources to facilitate the provision of health services; and
- exposure of the custodian as being negligent or ineffective in the discharge of its responsibilities through orders and reports of the Information and Privacy Commissioner and commentary from applicants, the media and interested members of the public.

Some common issues are outlined below.

Ability to Find Records

The right of access provisions of **Part 2** of the *Health Information Act* assume an ability on the part of custodians to identify, locate and produce records in response to requests. The search process is greatly facilitated if a retrieval system is in place that allows staff processing an access request to search for an identifiable individual's health information and find all locations where that information may be located.

The failure to capture health records in effective record-keeping systems may result in difficult and time-consuming searches for records, as well as uncertainty that all records relevant to a right of access request have been located. This is particularly an issue when no records can be found related to an individual, although it appears that a custodian should have created and maintained records about that individual and there is no evidence that the record was destroyed in an authorized manner.

An effective records management system should allow retrieval of semi-active as well as active holdings. It should also allow for retrieval of records in a storage facility, such as the Alberta Records Centre (for the department and for its agencies, boards and commissions under Schedule 1 of the FOIP Regulation).

In addition, the records management system should provide some ability to alert an applicant to the fact that his or her health records may have been transferred to the custodian's archives, if they have one.

Applicants may challenge the adequacy of a search for records by a custodian. It will be easier to demonstrate thoroughness if there is an established record-keeping system.

Custodians also need to be able to show that the search has been conducted in a systematic and reasonable manner and that all records reasonably related to an applicant's request have been located. In **IPC Order 99-021**, a department relied upon a previous search done in response to an earlier request from the same applicant and the opinion of an employee that no responsive records had been found at that time. The Commissioner stated that a search that relies on the memory of an employee is not in compliance with the *FOIP Act*.

Standard of Documentation

A custodian should have a standard of documentation. This requires clear direction as to how affiliates will document health records. Some examples of standard documentation practices are:

- writing legibly and accurately;
- recording concisely only the necessary information being as objective as possible and describing observations;
- recording events chronologically;
- dating all entries and signing or initialing them;
- recording the information immediately or as soon as possible;
- doing all documentation in ink, not pencil;
- correcting errors and omissions openly and honestly, including dating and initialing changes made;
- ensuring that warning/caution indicators on health records clearly stand out;
- supporting entries made to an electronic health record by codes indicating the identity of the person who inputted the entry and including the date and time of the entry; and

- following routine practices and procedures when recording health information.

Affiliates should be held accountable for documenting their activities and observations regarding the provision of health services. As well, there is a need in the modern electronic work environment to ensure that information technology systems have the capability to build in version control where this is required. This enables custodians to retrieve the authoritative versions of certain documents upon which actions or decisions are based.

There is also need for clear direction on what health records the custodian considers are transitory in nature. For example, rough notes, messages, and routine documentation, which have only short-term value, may be disposed of regularly at the discretion of an affiliate in accordance with a policy or guideline on transitory records.

In the absence of such direction on transitory records, the Commissioner could require a custodian to produce other evidence at an inquiry that a health record that has been destroyed was appropriately destroyed as a transitory record **(see IPC Order 99-009)**.

Transitory records are discussed in greater detail in section 11.2.4 of this Chapter.

Finally, standards of documentation should clearly indicate that the official health records of the custodian cannot be altered or destroyed without authorization.

Alteration or destruction of health records is a very serious matter, especially when done to evade a right of access request, and could lead to penalties or sanctions. **See section 9.6.3 of Chapter 9 of this Publication for information on the offence provisions of the Act.**

Controls over Disposition

Section 60(2) states that safeguards for the protection of health information must include appropriate measures for the proper disposal of records to prevent any reasonably anticipated unauthorized use or disclosure of health information or unauthorized access to health information following its disposal.

Section 108(1)(g) enables the Lieutenant Governor in council to make regulations respecting the retention, disposal and archival storage for records for the purposes of **section 60**. Regulations under this provision are currently being developed.

The *Act* does not prohibit the transfer, storage or destruction of a record in accordance with an enactment of Alberta or Canada **(section 3(c))**.

The requirements in **section 60(2) and section 3(c)** as well as cost-effective business practices dictate that a custodian have a systematic process for disposing of health records as they become inactive and are no longer needed for such things as providing health services, for health system management, for research or to protect the organization's interests in the event of litigation.

This process, known as records scheduling and disposition, has several advantages from the perspective of complying with the *Act*.

First, it provides control over the disposal or destruction of records, so that custodians know what was destroyed, and when. It also sets out what records of enduring value are transferred to archives. Establishment of retention and disposition schedules – and compliance with them – allows custodians to set accurate limits to searches for records.

Second, a schedule provides an official approval process for the disposition of health records after a fixed time period, including the destruction of transitory records, based on patient and organization needs. It provides evidence for the applicant, and for the Commissioner if necessary, that records have been appropriately disposed of by custodian.

In orders following reviews under the *FOIP Act,* the Commissioner has emphasized the importance of rules relating to the destruction of records, and he has noted that it is within the purview of the Commissioner to ensure compliance with such rules (**see IPC Order 98-011**).

Finally, a schedule allows for the movement of health records through the system. This reduces the need for custodians to tie up resources in the maintenance of older records, which may be very labour-intensive to locate and handle.

Older records that need to be permanently preserved to protect the interests of a custodian or the interests of patients (e.g. recipients of tainted blood products or breast implants) may be stored in the Provincial Archives of Alberta or in any other archival facility that is subject to the *Health Information Act* or to the *FOIP Act* (**section 38**). The reason for placing records in an archival facility is to permanently preserve the records or to allow for historical research. Before placing records containing individually identifying health information in an archives, the custodian must form the opinion that the information has enduring value.

See section 5.2.4 of Chapter 5 of this Publication for a discussion of the duty to protect health information and the requirements under section 60(2) of the *Act* and section 8.11 of Chapter 8 of this Publication for a discussion of disclosure of health information to an archives.

Right of access requests can then be dealt with by these organizations, which are usually well oriented to dealing with requests for records.

In summary, the lack of a systematic records scheduling and disposition system can mean that:

- older records are retained far longer than needed;
- there is random destruction of records, which can be embarrassing for the custodian or which may expose the custodian to risk of litigation;
- there is no official authority for the legitimate disposition of health records that are of no further use, including transitory records;
- resources may be wasted looking for records that no longer exist; and
- materials that should be permanently preserved may be lost.

Ability to Routinely Disclose Records outside the *Act*

A custodian needs:

- to have effective control over the health records and information which it creates and collects; and
- to be knowledgeable about such records and information.

This is required to make effective decisions about which records could be released on a routine basis, provided this is done in compliance with the *Act*.

11.2.3 RECORDS AND INFORMATION MANAGEMENT PRINCIPLES

The following principles underpin the effective management of health records.

The Management of Information is Planned

An organization's business planning processes require both strategic and operational records and information management planning.

All Records are Included

Management practices should apply to all records as defined in **section 1(1)(t)** of the *Act*, including electronic records. Electronic records include:

- electronic documents, such as word processed documents, spreadsheets, e-mail, web pages, graphics, digital photographs, and scanned images;
- electronic data, such as information stored in databases; and
- back-up tapes.

Electronic records include information in all media and in all locations. For example, electronic records may be stored on networks, local hard drives and portable hard drives, as well as in storage media such as floppy disks, CD-ROM disks, optical disks, and tape.

Information is an Important Resource of the Organization

An essential principle for the management of health records is that information is managed as a resource or asset of the whole organization and not as the property of affiliates or branches of a custodian.

A Life Cycle Management Approach is Adopted

Sound principles for the management of health records are based on the life cycle of information. Management activities within the life cycle encompass:

- the planning of information systems, including appropriate controls over the collection, creation or compilation of health information;
- the establishment of practices and procedures governing the organization, distribution, retrieval, use, accessibility and transmission of health records and for their storage, maintenance and protection;
- the provision for routine access to certain health information, as appropriate; and
- the regulation of the disposition of all health records.

Accountability is Assigned

Given the close relationship between the *Health Information Act* and the effective management of health records, there should be an assignment of accountability for the management of health records by an affiliate with sufficient experience and knowledge to carry out this responsibility appropriately.

11.2.4 RECORDS AND INFORMATION MANAGEMENT POLICY COMPONENTS

Policy and guidelines should govern the management of health records within a custodian's organization. These should be developed with the administration of the *Act* in mind and include appropriate references to information access and protection of privacy requirements in the policy statements as well as the procedures, practices and standards.

Beyond principles, certain basic requirements or policies should be set out relating to both the management of health records and the custodian's responsibilities under the *Act*.

The following components should be included in policies for the management of health records.

Life Cycle Management

The policy should require the custodian to plan, direct, organize and control health records throughout their life cycle, regardless of the form or medium in which the information is held.

The Establishment and Maintenance of Records Systems

Another component of a records and information management policy is for a custodian to establish a records system. A records system, which may be computerized or manual, is an information system which captures, maintains and provides access to health records over time.

A records system should be controlled by a current, comprehensive and structured identification or subject classification system. Such a classification system provides an effective means of organizing, locating and retrieving all health records in the custody or under the control of the custodian.

The records system should serve as a locator system for all holdings of health records. It should also indicate which department, branch or affiliate has responsibility for particular types of health records. In addition, it should support the application of privacy protection measures.

Guide to Information Holdings

An important component of a records system is the records inventory or guide to information holdings, which provides descriptions of the health records in the system.

The guide to information holdings is a critical tool for the overall management of health records. It should support access to information both internally, for the custodian's authorized purposes and externally, where such sharing is permitted by the *Act*.

The guide to information holdings may also serve as the basis for establishing records retention and disposition schedules.

The Creation and Generation of Records

The policy should establish effective controls over the creation, maintenance and use of all health records through the establishment of a documentation standard. This standard should indicate what health records need to be created and maintained. For example, records required for the provision of health services, or for legal, fiscal, audit, administrative or operational purposes should be maintained in a records system.

The standard of documentation should be understood and followed by all affiliates of a custodian.

A Guide for Transitory Records

The policy may enable affiliates to destroy transitory records. A transitory record is a record that does not have long-term value. Transitory records contain health information that is not required to meet legal, financial or other obligations, and has no historical value.

A full definition of transitory records that has been developed for provincial public bodies (subject to the *FOIP Act*) is provided in the publications **Records Scheduling and Disposition in the Government of Alberta, Chapter 2-9, and A Guide to Identifying and Disposing of Transitory Records, produced by Alberta Innovation and Science (Records and Information Management Services Branch).**

This definition would apply only to records held by provincial public bodies who are also custodians under the *Health Information Act*. Other custodians may develop and approve their own definitions, but must be prepared to defend deviations from recognized standards before the Information and Privacy Commissioner.

Certain types of recorded information are generally managed as transitory records:

- information of short-term value (e.g., notes kept to prepare official minutes of a meeting);
- duplicate documents;
- draft documents and working materials that are used to create a master record or that do not document changes in decisions;
- personal messages and announcements;
- e-mail that does not document a decision or transaction on behalf of the custodian. Custodians should have an internal e-mail policy that aids affiliates in deciding when electronic mail information should be retained in records systems; and
- voice mail that does not document a decision or transaction on behalf of the custodian.

The Organization, Storage and Protection of Recorded Health Information

An information management policy establishing a records classification system will provide a framework for the organization and storage of health records that facilitates the location and retrieval of those records or information in the records. The policy should also address information security and the protection of privacy of health information, both for the business of the custodian and for purposes of the *Act*.

The custodian should have standards in place relating to the organization, control, storage and protection of health information and health records, including electronic records. A regulation respecting the retention, disposal and archival storage of records for the purposes of **section 60** of the *Act* is being developed.

Special Rules for the Organization and Management of Electronic Records

Electronic records are subject to the *Health Information Act* and should be managed as part of any program for the management of recorded information.

Ideally, in an electronic records system, processes should be in place to ensure that, where necessary:

- individual records are uniquely identified;
- contextual data, or "metadata," relating to the specific record or transaction is preserved (this may consist of, for example, date, subject, names of correspondents or participants);
- records can be authenticated;
- there is version control;
- records are classified and indexed for retrieval;
- there are access controls;
- there are controls over the alteration of records, including audit trails on use; and
- there are processes in place to permit the disposal of obsolete records under approved processes and retention and disposition schedules.

An electronic records system should address the effective management, retention and disposal of e-mail.

If there is not an adequate electronic record-keeping system, the policy should require records to be printed off and managed as part of the record-keeping system applied to hard copy records.

The Planning of Electronic Information Systems

The application of new information technology within custodians often has an impact on existing record-keeping activities.

A records and information management policy may establish a mandatory process for introducing the records system requirements into the planning and design of electronic applications that will collect, create or generate health information used by the custodian.

Health information should be managed to promote individual access and, if individually identifying health information has been transformed to become non-identifying, to allow public access, where this is appropriate.

Privacy protection measures must be considered in the design and functional specifications for information systems that are used to collect, generate, manipulate, and disclose health information.

The particular requirements for protection of privacy of health information are discussed in Chapters 5, 6, 7 and 8 of this Publication.

The Scheduling and Disposition of Recorded Health Information

Control over the disposition of health records is an important aspect of records management that is critical to the administration of the *Act*. When responding to a right of access request under **Part 2** of the *Act*, it is necessary to know whether records have been destroyed and if so, whether this has been done in an authorized manner.

It is equally important to dispose of health records under conditions that protect the privacy rights of the individual **(section 60(2))**. Regulations under the *Act* respecting the retention, disposal and archival storage of records for the purposes of **section 60** are being developed and will be approved by the Lieutenant Governor in Council in due course.

A records retention and disposition schedule is a custodian's legal authority regarding how long health information of various types must be kept and how it is to be disposed of **(section 3(c))** either by destruction or archival preservation.

Each custodian should establish a scheduling process that governs the retention and final disposition of all the health information in its custody or under its control in accordance with any current regulations or authorities under which it acts or in future, under the regulation respecting the retention, disposition and archival storage of records for the purposes of **section 60**.

For example, currently, under the Records Management Regulation, the Alberta Records Management Committee approves records retention and disposition schedules for the department and its affiliated agencies, boards and commissions. The schedules provide authority to transfer records selected for archival preservation to the Provincial Archives of Alberta.

The scheduling process for provincial public bodies (under the *FOIP Act*) is discussed in the Alberta Innovation and Science publication Records Scheduling and Disposition in the Government of Alberta, Chapter 2-2.

For other custodians, authority to approve the transfer or destruction of health records will be derived from a governing body (e.g. a regional health authority or provincial health board, etc.) or from a health professional body pursuant to an enactment of Alberta or Canada.

For example, under the Operation of Approved Hospitals Regulation, made under the *Hospitals Act,* diagnostic and treatment service records must be retained by the hospital for the following periods:

- a period of 10 years from the date of discharge from hospital;
- in the case of a patient being a minor, for a period of at least 2 years following the date on which the patient reached the age of 18 years; and
- diagnostic and treatment service records may be retained by the hospital for an additional period as my be considered necessary by the board.

Also, under the above Regulation, diagnostic and treatment service records:

- may be microfilmed on discharge of the patient from the hospital and the original records may then be destroyed after one year from the date of discharge of the patient; and
- x-ray films may be destroyed after 5 years from the date of discharge of the patient.

Another example of retention and disposition schedules can be found in the **College of Physicians and Surgeons of Alberta bulletin on "Physician's Office Medical Records"**. In that bulletin, the recommended retention schedules for x-ray films, mammography films and x-ray reports are set out.

In addition, the Council of the College recommends that physicians retain their office medical records for a minimum period of ten years, or in the case of minor patients, until two years after the age of 18 or for 10 years, whichever is longer. This includes retention by electronic means or storage of hard copy, the entire interpretive report and a segment of continuous physiologic recordings, whether abnormal or not, sufficient to support the interpretation made.

Following these periods of availability, records may be disposed of by secure and confidential shredding, burning or erasing. Commercial shredding services are available.

Sections 15, 16, 17 and 18 of the Pharmaceutical Profession Regulation under the *Pharmaceutical Profession Act* establish retention and disposition practices for pharmacists. For example, prescription records must be kept for 2 years after the last change to a prescription.

Custodians must pay strict attention to disposal processes for health records. Disposal processes should be governed by established and well-understood procedures and be carried out in accordance with the regulation under the *Health Information Act* (being developed).

Sensitive health information intended for destruction but left in insecure condition may be exposed to unauthorized access and, possibly, use. Examples include disposal of garbage bags that rip open and release documents containing health information, and disposal of health information in a recycling container.

Used office and computer equipment poses a special risk. In one investigation under the *FOIP Act* by the Information and Privacy Commissioner, filing cabinets were found to have been moved to an auction centre with files containing personal information still inside. Computer hard drives have been similarly put up for auction with information still stored on them. In another example of inappropriate disposal, inactive health records were found in an open area of a hospital by workers demolishing the hospital.

Pulping or shredding is the best way of disposing of paper and other hard copy media. This should be done in a facility or by a mobile shredding service that can ensure complete and secure destruction.

At a minimum, computer hard drives and diskettes need to be professionally wiped clean of data before they are disposed of or sold.

For surplus computers, the department must:

- remove data from hard drives and diskettes and verify that the data has been removed prior to shipping to Surplus Sales. It must also verity that after wiping, no data is accessible using disk analysis tools such as Norton's Utilities Disk Editor;
- remove external media such as tapes, CD's diskettes and ZIP disks from computers prior to shipping to Surplus Sales. If the media is to be destroyed, the department must follow the procedures outlined in the Records Scheduling and Disposition in the Government of Alberta publication;
- for disk wiping, use commercial or in-house software that writes random characters over the entire hard drive and is shown, using disk analysis tools, not to leave any trace information;
- remove and destroy hard drives that cannot be completely cleared of data; and
- provide a certification of data removal report prior to shipping the computer to Surplus Sales.

See the Alberta Innovation and Science Policy for Maintaining Security of Government Data Stored on Electronic Data Storage Devices (November 1999) and the update (January, 2001) entitled Security Policy for Disk Wiping Surplus Computers.

For custodians who are also public bodies subject to the Records Management Regulation, destruction of recorded information must take place in accordance with the records management policies and procedures established by the Government of Alberta. Alberta Infrastructure, Surplus Sales, offers services to these public bodies for the wiping clean of computer hard disks before their disposal.

Records Management in Contracting

For programs and services contracted by custodians to other agencies, provision should be made in policy for all contracts to require the contractor to create records that meet the custodian's requirements. Contracts should also require the contractor to maintain health records according to standards acceptable to the custodian for as long as required, to dispose of the records according to standards acceptable to the custodian, or to return the records to the custodian, as appropriate.

When activities requiring the collection or handling of health information are contracted out, the contract should set out the privacy protection and security obligations assumed by the contractor (**see Chapters 5, 6, 7 and 8 of this Publication**).

11.3 PRIVACY, INFORMATION MANAGEMENT AND SECURITY

Parts 3 to 6 of the *Act* establish the rules regarding the collection, use, disclosure, disposal and protection of health information. The following sections of this Publication provide some guidelines to help custodians:

- review their information systems and practices to bring them into compliance with **Parts 3 to 6** of the *Act* **(Collection, Use and Disclosure of Health Information and Powers and Duties of Custodians Relating to Health Information)**;
- review forms used in the collection of health information to ensure that they meet the collection and notification requirements of the *Act*;
- conduct threat and risk assessments to identify potential threats to or vulnerabilities affecting the security of health information and to assess the level of risk and the impact of identified security breaches; and
- develop a security policy that supports protection of health information privacy.

11.3.1 REVIEWING COMPLIANCE WITH PARTS 3 TO 6 OF THE *ACT*

This section provides a checklist to assist custodians in reviewing their compliance with the rules regarding the collection, use, disclosure, disposal and protection of health information in their custody or under their control as set out in **Parts 3, 4 and 5** of the *Act* as well their duties and responsibilities under **Part 6.** This is the same checklist that is used in the technical compliance portion of the privacy impact assessment process and can be used for both automated and manual information systems.

The responses to the following questions/criteria will help a custodian determine whether it is in general compliance with the requirements of **Parts 3 to 6** of the *Act* for each of its information systems or programs.

1. Collection of Health Information (Sections 19 & 20)

- Is individually identifying health information being collected?
- What is the authority for the collection?
  - Is the collection expressly authorized by an enactment of Alberta or Canada? **(section 20(a))**
  - Does the information relate directly to and is it necessary to carry out a **section 27** purpose? **(section 20(b))**

- Has only necessary health information been collected (on a need to know basis)? **(section 24)**
- Is the information being collected at the highest level of anonymity possible and in a limited manner? **(sections 57 and 58)**

2. Collection of Personal Health Number (Section 21)

- What authority requires individuals to provide their personal health number (PHN) (if this needs to be collected)?
  - Is the person requiring provision of the PHN a custodian or a person authorized by section 4 of the *Health Information Act* Regulation? **(section 21(1))**

3. Manner of Collection of Health Information (Section 22)

- Is individually identifying health information collected directly from the individuals it is about? **(section 22(1))**
- How will affected individuals be notified of the legal authority for and purpose(s) for the collection as well as the contact information? **(section 22(3))**
- If individually identifying health information is being collected indirectly, what is the authority for the indirect collection and what is the source?
  - What exception to direct collection applies under **section 22(2)**?

- Is the information flowing from another custodian or another system?
- If there is a linkage to another database is it on a one time only or on an ongoing basis? **(see questions in #15 below on Data Matching)**
- Are there procedures in place to periodically review the need for the information (e.g. 5 years or with a change in the program or service)?

4. Use of Health Information (Sections 27-30)

- Is individually identifying health information being used?
- Have all the anticipated uses been identified and are they authorized uses under **section 27**?
- If the personal health number has been collected, is it only being used for the purpose for which it was collected? **(section 30)**
- Is the health information being used at the highest level of anonymity possible and in a limited manner? **(sections 57 and 58)**
- Is the health information only being used by those who have a need to know? **(section 28)**
- Has a reasonable effort been made to ensure that the information being used is accurate and complete? **(section 61)** **(See #12 in the Checklist regarding Duty to Ensure Accuracy of Health Information)**

5. Disclosure of Health Information (Sections 34–45)

- Is individually identifying health information being disclosed?
- Will this be an ad hoc or one-time disclosure of information or will the disclosure be on a planned (or regular) basis?
- Who will the records containing this information be disclosed to or who will have access to them? Will they have full access or limited access?
- Is a new record containing health information created as a result of the disclosure (e.g. as a result of data matching)?
- If disclosure of individually identifying health information is done with consent of the individual, does the form of consent meet the requirements of **section 34(2)**?
- Have all the anticipated disclosures of individually identifying diagnostic, treatment and care information without consent been identified and authorized under **sections 35 or 39**?
- Is information on disclosures of records containing individually identifying diagnostic, treatment and care information maintained (disclosure notations)? **(section 41)**
  - Are the disclosure notations retrievable by individual identifier to support an individual's right to access this information?
- Have all the anticipated disclosures of registration information without consent been identified and authorized under **section 36**?
- Have all the anticipated disclosures of health services provider information without consent been identified and authorized under **section 37**?
- If there is an anticipated disclosure of individually identifying health information without consent to the Minister, is there authority to disclose under **section 40**?
- How will the recipient of individually identifying diagnostic, treatment and care information be notified of the purpose of the disclosure and the authority under which the disclosure is made **(section 42)** if the disclosure is to a person or organization other than those in **section 42(2)**?
  - If the recipient is a non-custodian, has the recipient been notified not to use the information for data matching purposes without notifying the Commissioner? **(section 32(2))**
- How will the custodian disclosing the health information ensure that the person to whom the disclosure is made is the person intended and authorized to receive the information? **(section 45)**
- Is the health information being disclosed at the highest degree of anonymity possible and in a limited manner? **(sections 57 and 58)**
- Is the health information only being disclosed to those who have a need to know? **(sections 43 and 58(2))**

6. Disclosure to Minister or Department for Health System Purposes (Section 46)

- If individually identifying health information is being disclosed by a custodian to the Minister or the Department, is there authority to disclose under **section 46(1)**?
- Is the Minister or department authorized to obtain the information under an enactment of Alberta or Canada? **(section 46(1)(a))**

  - Does the requested information relate to a health service provided by the other custodian that is fully or partially paid for by the department, or that is provided using financial, physical or human resources provided, administered or paid for by the department? **(section 46(1)(b))**

- Is there authority for the Minister or department to disclose this information to another custodian? **(section 46(4))**
- If the information to be disclosed to the Minister or department relates to a health service provided by the other custodian under **section 46(1)(b)**, has the required Privacy Impact Assessment been completed and have the comments of the Commissioner been considered? **(section 46(5))**

7. Disclosure to Health Authorities, Alberta Cancer Board and Alberta Mental Health Boards (health authorities) for Health System Purposes (Section 47)

- If individually identifying health information is being disclosed to health authorities under **section 47**, is there authority for that disclosure under **section 47**?
  - Is the health authority requesting the information authorized to obtain the information under an enactment of Alberta or Canada? **(section 47(1)(a))**
  - Does the requested information relate to a health service provided by the other custodian that is fully or partially paid for by the health authority, or that is provided using financial, physical or human resources provided or administered by the health authority? **(section 47(1)(b))**

- Has the custodian receiving the request refused to disclose the information? **(section 47(2))**
  - Has the custodian who refused the request disclosed non-identifying information to the requesting custodian? **(section 47(3))**
  - Has the health authority asked the Commissioner to review the refusal? **(section 47(4))**

- Is there authority for the health authority receiving the information to disclose this information to another custodian, to the Minister or to the department under **section 47(5)**?

8. Disclosure By Electronic Means? (Section 59)

- If individually identifying diagnostic, treatment and care information is being disclosed by computer systems that facilitate access by authorized persons to electronic or digital information that is stored in a computer database by a custodian, have the individuals who are the subjects of the information consented to disclosure by electronic means in accordance with **section 59**?
  - Has the custodian obtained consent or ensured that consent is in place? **(section 59(1))**
  - Does the form of consent meet the requirements of **section 59(2)**?

9. Disclosure for Research Purposes (Sections 48 – 56)

- If the disclosure is for research purposes, have the requirements in **sections 49 – 56** been complied with?
- Has a proposal from a researcher been received and reviewed by an ethics committee under **sections 49 and 50**?

- Has the ethics committee recommended disclosure of the information to the researcher; has the committee imposed certain conditions on the researcher; have the necessary consents, if any been obtained? **(section 50(3))**
- Has the researcher applied to the custodian for disclosure of the health information to be used in the research and provided the response of the ethics committee to that custodian? **(section 52)**
- Has the researcher entered into an agreement with the custodian in accordance with **section 54**?
- If there is a need to collect additional health information, has the custodian obtained consents from the individuals to be contacted by the researcher **(section 55)**?
- If the disclosure for research purposes involves data matching of individually identifying diagnostic, treatment and care information or individually identifying registration information, have the provisions in **sections 48 to 56** been complied with **(section 72)**, including the conducting of a privacy impact assessment? **(sections 64, 32(2), and 71)**

Note that the definition of "health information" in **Division 3** of the *Act* **(Disclosure for Research Purposes)** refers to individually identifying diagnostic, treatment and care information or individually identifying registration information, or both. It does not include individually identifying health services provider information. Even though an ethics committee review may have been conducted under **section 50**, the disclosure of individually identifying health information for data matching for research purposes would still require a Privacy Impact Assessment (PIA) to be conducted **(section 72)**. However, the portions of the assessment done by the ethics committee related to security safeguards could be used in the PIA.

10. Right of Individual to Access Health Information (Section 7)

- Are procedures in place to ensure that an individual can review a record containing that individual's health information? **(section 7)**

- When an individual challenges the denial of access to a record, are they provided with information about their rights of recourse (e.g. right to request a review by Commissioner? **(section 73)**

11. Right of Individual to Request Correction or Amendment of Health Information (Section 13)

- Will the system incorporate a process to accommodate requests for correction or amendment under **section 13**?
- Does the system include disclosure audit trails or logs to determine who may have previously relied on incorrect information?
- When an individual challenges the accuracy of a record, are they provided with information about their rights of recourse (e.g. right to request a review by Commissioner)? **(section 73)**

12. Duty to Ensure Accuracy of Health Information (Section 61)

- Has a reasonable effort been made to ensure that the information being disclosed is accurate and complete? **(section 61)**

- Is there a system of verification for health information collected and for its entry on the system?
- Does the record indicate the last update date?
- Is a record kept of the source of the information used to make changes (e.g. paper or transaction records)?
- Is there a process in place to grant staff authorization to add, change or delete personal information from records held by the system?
- Is there a procedure for correcting or amending the information in the record?
- Does the system have the necessary audit trails to determine who may have previously relied on the incorrect information?
- Are procedures in place for disposition of health information and are actual records retention and disposition schedules agreed upon and signed for all the information in the system? **(section 60(2))**

13. Duty to Protect Health Information (Section 60)

- Have reasonable steps been taken, in accordance with section 8 of the Health Information Regulation and with **section 60**, to maintain administrative, technical and physical safeguards to ensure the protection of health information? **(section 60(1)(a) and section 8(1) and (3)** of the Health Information Regulation)
- If health information is going to be stored or used in a jurisdiction outside Alberta or disclosed to a person in a jurisdiction outside Alberta, how will the confidentiality of that information and the privacy of individuals who are the subject of that information be protected? **(section 60(1)(b))**
  - Is there an agreement in place as required under **section 8(4)** of the Health Information Regulation? (Note that an agreement is not required when an individual's health information is used outside Alberta solely for providing continuing treatment and care to the individual) **(section 8(5)** of the Health Information Regulation)

- Is there a responsible official who has the security authority for the system or administrative practice? **(section 8(2)** of the Health Information Regulation)
- Has there been an expert review of all the risks and vulnerabilities as well as the reasonableness of the proposed safeguards to protect health information against unauthorized or improper access, collection, use, disclosure and disposal of the information? **(section 60(1)(c) and section 8(3)** of the Health Information Regulation)
- Are there documented procedures for collecting, processing, accessing, transmitting, storing and disposing of the health information? **(section 63 and section 8(1)** of the Health Information Regulation)
- Have affiliates been trained in requirements for protecting health information and are they aware of policies regarding breaches of security or confidentiality and sanctions for unauthorized collection, access, use or disclosure of health information? **(section 60(1)(d), section 63 and section 8(6), (7)** of the Health Information Regulation)
- Are written policies and procedures in place related to the protection of individual privacy and confidentiality of an individual's health information with respect to each information system/program or service? **(section 63**

and sections 8(1), (6), (7) of the Health Information Regulation)

- Are there controls in place over the process of who receives authority to add, change or delete health information from records? **(section 60(1)(a) and (c))**
- Is the system designed so that access and changes to health information can be audited by date and user identification? **(section 60(1)(a) and (c))**
- Are access rights only provided to users who actually require access for the stated purposes of collection? **(section 60(1) (a) and (c))**
- Is user access to health information limited to only that required to discharge the assigned functions? **(section 60(1) (a) and (c))**
- Are the security safeguards commensurate with the sensitivity of the health information and its vulnerability to compromise? **(section 60(1)(c) and section 8(3)** of the Health Information Regulation)
- Are there appropriate physical security measures such as security access zones, locked rooms, storage cabinets; controlled access to computer terminals and faxes to prevent random access; checkout and secure transmission procedures for files? **(section 60(1)(a) and (c), and section 8(1), (3)** of the Health Information Regulation)
- Are there contingency plans and mechanisms in place to identify security breaches or disclosures of health information in error? **(section 8(7)** of the Health Information Regulation)
- Is health information retained for purposes other than that for which it is collected?
  - Explain the reasons for retention, the form of retention and controls over disposal **(section 3(c))**
  - Are procedures in place for the disposal of health information, including information in electronic form, which protect it from unauthorized disclosure until disposal is completed? **(section 60(2))**

- Is there any monitoring and review of the general effectiveness of the security measures/safeguards? **(section 60(d) and sections 8(2) and (4)** of the Health Information Regulation)

14. Contracted Services

- Is the health information collected, used or disclosed to contractors in carrying out programs or services or is it managed by contractors on behalf of the custodian?
  - Have all affiliates who are contractors been identified?
  - Do the contractors understand that they must comply with the *Act* and regulations under the *Act* and the policies and procedures established or adopted under **section 63**?

- Does the contract bind the contractor to comply with the *Act* & regulations under the *Act* and the policies under **section 63**?
- Is the contractor acting as an "Information Manager"? **(section 66)(1))**
  - Is there an agreement in place with the Information Manager in accordance with the regulations? **(section 66(2))**
  - Is the Information Manager's compliance with the *Act* and regulations under the *Act*, the conditions of the agreement and the authorized purposes for disclosure being monitored? **(s. 66(4) &(5))**

15. Data Matching

- Is individually identifying health information being collected for the purpose of data matching? Is it being used or disclosed for data matching purposes or is it being created as a result of data matching? Is there authority for the collection, use or disclosure of the information and is the data matching being performed in compliance with the *Act*? **(section 68)**
- Is the information that is being used for data matching in the custody or under the control of the custodian who is using it? **(section 69)**
    - Is there a data matching policy and guidelines in place within the custodian? Have they been followed?
    - Has the data matching been authorized by an appropriate designated official within the custodian?
    - Has information generated or created by the matching program been verified against original or additional authoritative sources before the information is used for an authorized purpose, especially if it impacts an individual?

- Is the information in the custody or under the control of one custodian being combined with information that is in the custody or under the control of another custodian? **(section 70)**
    - Is there a data matching policy and guidelines in place within the custodian? Have they been followed?
    - Has the data matching been authorized by an appropriate designated official within the custodian?
    - Has information generated or created by the matching program been verified against original or additional authoritative sources before the information is used for an authorized purpose, especially if it impacts an individual?
    - Has the custodian who will be storing the information created through data matching conducted a Privacy Impact Assessment and submitted it to the Commissioner for review and comment, meeting the requirements of **section 70(3)**? Does it include an assessment of the advantages of the proposed matching against alternative control, management or enforcement approaches; and an assessment of how the information is to be collected and how the information created through data matching is to be used or disclosed? **(sections 70(2) and (3))**

- Is the information in the custody or under the control of a custodian being combined with information that is in the custody or under the control of a non-custodian? **(section 71)**

    - Is there a data matching policy and guidelines in place within the custodian? Have they been followed?
    - Has the data matching been authorized by an appropriate designated official within the custodian?
    - Has information generated or created by the matching program been verified against original or additional authoritative sources before the information is used for an authorized purpose, especially if it impacts an individual?

- Has the custodian conducted a Privacy Impact Assessment and submitted it to the Commissioner for review and comment, meeting the requirements of **section 71(3)**? Does it include an assessment of the advantages of the proposed matching against alternative control, management or enforcement approaches; and an assessment of how the information is to be collected and how the information created through data matching is to be used or disclosed? **(sections 71(2) and (3))**
- If the data matching is performed for the purpose of conducting research, have **sections 48-56** been complied with before the data matching is performed? **(section 72)**

11.3.2 REVIEW OF FORMS

When individually identifying health information is collected directly from the individual that it is about, **section 22(3)** of the *Act* requires that the individual be notified of the purpose for which personal information is being collected from him or her, the specific legal authority for the collection, and the title, business address and telephone number of someone who can answer questions about the collection.

Forms are a major way of collecting personal information. For that reason, it is important to bring forms (paper and electronic) into compliance with the provisions the *Act*.

In doing so, custodians will:

- support the right of individuals to know what health information custodians collect about them and how this information is used;
- support the right of individuals to access information about themselves; and
- help maintain confidence among individuals that custodians are protecting their personal information from unauthorized collection, use and disclosure.

As indicated in **Chapter 6 of this Publication,** achieving compliance with the collection requirements set out in **sections 21 through 24** as well as with the duties of custodians under **sections 57, 58, 60, 61, and 64** of the *Act* requires a thorough review of a custodian's collection activities. Included in this should be a review of all forms to ensure that those used to collect information directly from individuals meet the requirements of the *Act* and that any unnecessary forms are eliminated.

This may be a process of some magnitude for custodians that have a large amount of health information in their custody or under their control. Some of this work may have already been done for custodians that are also public bodies under the *FOIP Act* but should be reviewed to ensure that the forms still comply with the *Act.*

For custodians who have not conducted a review of forms for the purposes of complying with the *FOIP Act,* the process will likely be planned and implemented over time, often on a program or service basis or as part of re-engineering and system development activities.

Revisions should be considered when there is a need to reprint or redesign forms. There should also be a priority list of significant forms that need revision as soon as possible. This may be because of the volume of health information collected on these forms, or the extent to which the particular forms are used.

Where necessary, custodians should make interim arrangements to ensure that individuals receive the notification (or privacy statement) required under **section 22(3)** when health information is collected directly from them. This may be done by printing supplementary sheets containing a privacy statement to go with the forms, or by producing a short brochure or bulletin that explains the privacy protection being offered by the particular program or custodian. Computer-based forms can be updated with a notification almost immediately.

To facilitate notification, custodians may print a supply of notifications (or privacy statements) covering:

- the purpose for which the information is collected;
- the legal authority for collection;
- the uses to which the information will be put; and
- the name, business address and telephone number of a person who can answer questions about the collection.

These may be provided separately to individuals or attached to or contained in the forms being provided to individuals.

In cases where some health information on a form should no longer be collected (e.g. there is no need to collect it), custodians should inform clients/patients that certain fields must not be filled out. These instructions should be provided in writing, and affiliates should take steps to achieve consistency in their approach to handling forms. In some instances, it may be possible to black out fields that are no longer required.

A review of forms and other collection instruments may be combined with the review of compliance with **Parts 3 to 6** of the *Act* discussed in **section 11.3.1 of this Chapter.**

Notification

The notification may be printed on the collection form itself, on a separate or covering document that explains the form and how to fill it out, or it may be given verbally. Oral notification is practical when information is taken personally over the telephone, given by touch-tone telephone or taken during an interview.

When the notification is provided orally, care must be taken to provide the individual with a copy of the privacy statement either at the office where collection takes place or with the documentation sent to an individual to confirm collection of information over the telephone or electronically.

An example of a collection notification is as follows:

"This personal information is being collected under the authority of (state name of act or program) and will be used to (state known purposes). It is protected by the privacy provisions of the Health Information Act . If you have any questions about the collection, contact (name, address, and business telephone number of responsible affiliate)". **(See the Sample Collection Notice in Appendix 1 of this Publication)**

Optional Practices

There are a number of practices for the collection of health information through forms which reflect good management of health information but are not mandatory under the *Health Information Act*.

EXAMPLES OF OPTIONAL BEST PRACTICES INCLUDE:

- *design of forms to ensure that the individual from whom the information is collected is given a copy of the notification;*
- *design of forms to ensure that a copy of the notification is also retained by the custodian;*
- *detailed notifications where appropriate to inform the individual about his or her right to request correction of inaccurate or incomplete information, the right to appeal refusals of corrections and the role of the Information and Privacy Commissioner in reviewing such refusals;*
- *review by the Health Information Coordinator or responsible affiliate of all new forms and proposed revisions before finalization for printing, including review of privacy issues; and*
- *where personal information is collected from a source other than the individual the information is about (indirect collection), provisions to inform individuals generally that information about them is being sought from a variety of specific sources. Such explanations should be included in documentation or brochures given to individuals who are the subjects of the indirect collection.*

Electronic Forms

There are a number of special factors that should be taken into consideration when dealing with computer-generated forms or when planning to move into an electronic forms environment.

BEST PRACTICES INCLUDE:

- *a policy and accountability structure should be put in place to ensure that privacy statements are included on electronic forms, which are often generated on a decentralized basis;*
- *when software for creating forms is under consideration, one of the specifications should be that it permits the easy addition of collection notifications or privacy statements in ways that are convenient and that effectively inform the individual filling out the electronic form of his or her privacy rights;*
- *provision should be made for authorization of indirect collection and for authorization of additional uses or disclosures of the information on electronic forms where this is permitted under the Act, as well as for a signature or other verification of the identity of the individual providing the authorization;*
- *a hard copy of the form should be provided to the individual the information is about, including the notification of collection (privacy statement) on the form; and*
- *the custodian should be able to retain a copy of the authorization and notification.*

These practices establish an audit trail within electronic information collection for the authorization of collection, the source of the information and the notification of collection and use. If these practices are not used, some other audit practices should be in place.

Review Process

The following practices can assist in bringing existing forms into compliance with the *Act*:

BEST PRACTICES INCLUDE:

- *since the revision of forms may be a significant task, establish a plan which stretches over several years for revision;*
- *concentrate first on those forms used to collect information directly from individuals and choose the most visible or most used forms in this category for early review and revision. Leave other changes that are optional and not mandatory under the Act until later;*
- *carefully review and refine the notification statement to be included on or attached to the form and integrate the statement into the design of the form;*
- *establish a process where new forms can be quickly reviewed to ensure they meet the privacy standard established by the custodian;*
- *include the requirements of the Act in the normal forms review process;*
- *keep stocks of all forms used to collect personal information at minimum levels pending review; and*
- *make revisions to forms at normal reorder points to avoid special printing runs.*

Interim measures may be set up pending forms revision:

- *train affiliates that receive forms containing health information over the counter on how to give a verbal notification that meets the requirements of the Act and provide statements indicating that the privacy provisions have been explained;*
- *prepare a supply of photocopied notifications covering the purpose for which the information is collected, the authorization for collection and the uses to which the information will be put, and provide these to clients or attach them to the forms being provided to individuals; and*
- *establish and maintain an inventory of forms used for the direct collection of personal information and establish a monitoring function to detect forms that do not include the appropriate notification.*

11.3.3 CONDUCTING A THREAT AND RISK ASSESSMENT

In order to determine the level of protection of health information that is needed to comply with **section 60** of the *Act* and **section 8** of the Health Information Regulation, a threat and risk assessment needs to be conducted for the health information held by the custodian as a whole and also for the health information needed for each key function, program or service within or provided by a custodian. This process should be flexible and ongoing with the ability to identify new risks as they arise. Threats will change continuously so that current threats will need to be re-evaluated and potential or anticipated threats identified. Re-assessment will also be needed as the nature of health information in the custody or under the control of a custodian changes or as new safeguards are developed.

Framework for a Threat and Risk Assessment

The components of a threat and risk assessment are as follows:

- Determine what health information and other assets are to be protected.
- Determine what threats there are to the privacy of individuals who are the subjects of the health information in the custody or under the control of the custodian and to the confidentiality of that health information.
- Assess whether existing or proposed security measures or safeguards are adequate and determine vulnerabilities.
- Identify what steps should be taken to manage the identified risks.

Determine What Health Information and other Assets are to be Protected

Health information in the custody or under the control of the custodian can be grouped according to the function, process, program or service it supports. Within each group, the information may have different requirements for its protection. As part of this determination, the data items or information, software, staff (users, administrators, analysts), storage facilities, storage media, system documentation, etc. should all be listed.

Determine the Potential Threats to the Security of Health Information

For each grouping of health information:

- identify the potential agents or events that could place the asset or group of assets at risk (e.g. theft, unauthorized access, viruses, power loss, etc.);
- classify each agent or event by the type of threat;
- determine how likely the event is to occur; and
- identify the potential consequences and rate the impact of the events if they were to occur.

Threats to the security of information include threats to its confidentiality, integrity and availability. Common threats are:

- disclosure of information – e.g. unauthorized verbal disclosure, leaving information displayed on a monitor, electronic interception of information travelling over a transmission line, such as a fax machine or cellular phone, faxing information to the wrong fax number, unauthorized access to information stored on an affiliate's home computer;
- service interruption – e.g. power failure, labour dispute, denial of service attack on an Internet server;
- modification of data – e.g. malicious code, forgery, addition of data to a record;
- accidental or deliberate loss of data – e.g. physical damage to hardware, willful destruction of recorded information, information destroyed in a flood or fire;
- removal of equipment – e.g. theft of a laptop or file containing health information, use of information outside the custodian's office (e.g. using the information on a home computer), disposal of information at the custodian's home;
- misuse of information – e.g. transfer of or sale of health information in contravention of the *Health Information Act*; and
- information not being available – e.g. records that are misdirected or misfiled, or that are destroyed in a manner that is not in accordance with approved records

retention and disposition schedules or policies.

Determine the likelihood (low, medium or high) of each or any of the above threats occurring. Identify the potential consequences and rate the seriousness (less serious, serious or very serious) of the events if they were to occur.

Assess Whether Existing or Proposed Security Measures or Safeguards are Satisfactory

Based on the potential threats that have been identified and the likelihood and impact of the events occurring that could place each group of health information at risk, assess the adequacy of existing safeguards and current resources to protect against the potential threats.

This assessment involves listing the existing safeguards to protect against the potential event; considering whether the information might still be vulnerable to the potential threat; and rating the potential risk. A low risk potential will require some attention and consideration for safeguard implementation; moderate risk potential requires attention and safeguard implementation in the near future; and high risk potential requires immediate attention and immediate safeguard implementation.

Identify the Steps to Take in Managing the Identified Risks

In considering potential vulnerability and risk, identify any additional safeguards recommended to lower the risk to an acceptable level and describe those proposed measures or safeguards.

Different safeguards may provide different levels of protection. Selection of the most appropriate safeguard will depend upon the availability of resources, and the acceptable level of risk. Custodians can rate the projected risk if the proposed safeguard was to be put in place as low, moderate or high. However, keep in mind that implementing the 'high' safeguards may not be practical depending upon technical or physical limitations or upon time or financial constraints.

This Framework for Conducting a Threat and Risk Assessment was adapted from the *Guidelines for Computer Security at Central Queensland University in Australia* which was adapted from *The Security and Privacy Guidelines for Health Information Systems (1995, COACH, Edmonton)* which was adapted from the RCMP *Threat and Risk Assessment for Information Technology.* See also Threat and Risk Assessment Guidelines (http://www.gov.ab.ca/sharp)

11.3.4 DEVELOPING A SECURITY POLICY

Section 60(1) requires a custodian to take reasonable steps in accordance with the regulations **(see section 8** of the Health Information Regulation) to maintain administrative, technical and physical safeguards that will:

- protect the confidentiality of health information in its custody or under its control and the privacy of the individuals who are the subjects of that information;
- protect the confidentiality of health information that is to be stored or used in a jurisdiction outside Alberta or that is to be disclosed by the custodian to a person in a jurisdiction outside Alberta and the privacy of the individuals who are the subjects of that information;

- protect against any reasonably anticipated:
    - threat or hazard to the security or integrity of the health information or of loss of the health information, or
    - unauthorized use, disclosure or modification of the health information or unauthorized access to the health information; and
- otherwise ensure compliance with the *Act* by the custodian and its affiliates.

Section 60(2) says that the safeguards to be maintained must include appropriate measures for the proper disposal of records to prevent any reasonably anticipated unauthorized use or disclosure of the health information or unauthorized access to the health information following its disposal.

See the discussion on Duty to Protect in section 5.2.4 of Chapter 5 of this Publication.

As an important means of ensuring compliance with the duty to protect health information under the *Act,* a custodian should establish a health information security policy, make its affiliates aware of the policy and require them to adhere to it. The policy should set out the usual practices and procedures of the custodian aimed at maintaining the administrative, technical and physical safeguards deemed to be necessary from the threat and risk assessment conducted by the custodian.

The following components for a health information security policy are adapted from the *Canadian Organization for the Advancement of Computers in Health (COACH) Guidelines*.

Authority

The policy should contain a statement of the authority or authorities under which it is being issued and a direction from the senior officer of the custodian on its effective implementation.

Administrative and Organizational Security

This part of the policy will set the overall framework and should include:

- having a written health information security policy;
- specifying the responsibility of the person responsible for the policy;
- specifying the purpose(s) of each information system operated by the custodian;
- setting a schedule for review and audit activities, including responsibilities and threat and risk analyses;
- setting out the processes and procedures for patients to access their own health information; and
- establishing information system access records and setting out schedules and processes for retention and disposal of such records.

Personnel Security

This part of the policy ensures that personnel are aware of security requirements and should include:

- recruitment policies, including the requirement for a signed and witnessed oath or pledge of confidentiality and privacy;
- training requirements for new and existing staff regarding the *Health Information Act* and the confidentiality and privacy requirements;

- mechanisms for determining each affiliate's level of 'need to know' and procedures for restricting that affiliate to an appropriate level of information access;
- policies regarding appropriate separation of duties (e.g. affiliates providing health services shouldn't be able to change the information operating system and affiliates who are information systems staff shouldn't be accountable for input errors);
- policies and procedures for personnel identification, ensuring that each person is uniquely identified to the information system and to others in the working environment;
- mechanisms for control (distribution, replacement and retrieval) of personnel security-related items (e.g. keys and other access material, passwords, user ID's, ID badges, etc.); and
- consequences of violating the security policy (e.g. disciplinary action, loss of privileges, legal action, etc.).

Physical and Environmental Security

This part of the policy focuses on the physical plant and the security risks and hazards in that location and should include:

- periodic reviews of physical security features (e.g. fences, walls, alarms, access and egress routes, surveillance devices, etc.);
- policies and procedures for designation of secure areas, access controls to those areas, designation of authorized users of those secure areas, and maintenance of access control logs to secure areas;
- establishing standard operating procedures for the installation, monitoring and maintenance of environmental support equipment, communications and electrical wiring and equipment, plumbing and other utilities and services;
- specifying adequate fire and fire safety procedures;
- designating off-site storage facilities with a similar level of physical and environmental security; and
- evacuation procedures in case of physical or environmental hazards.

Hardware Security

This area ensures that hardware is made secure from inappropriate access, accident, misappropriation and systems failure and should include:

- adequate virus protection for new and existing equipment;
- specifying system security features (e.g. passwords are not displayed, automatic power-down of unattended equipment, user authentication procedures, hardware error logs, etc.); and
- establishing hardware maintenance and support schedules, including support facilities (e.g. power supply).

Communications Security

This area relates to all forms of communications, including voice (speaking in person), written documents, fax, e-mail, video and audio (radio) communications, land-line telephones, cellular phones, and other forms of electronic communications and should include:

- specifying the security features in each type of communication system used by the custodian;
- establishing communication systems maintenance and support requirements and schedules;
- establishing security controls for remote access to information systems; and

- restricting the use of less secure forms of communications (e.g. fax and cellular telephones).

Software Security

This area relates to security issues involved in the purchase, installation, use and disposal of systems software and should include:

- specifying the system development life cycle methodology used by the custodian;
- committing to respecting copyright of purchased software;
- quality assurance and user acceptance testing procedures for newly purchased or developed software;
- procedures for software library control and software access control;
- specifying software security procedures, including use of passwords, termination on inactivity, clearance of display screens, transactions logs, integrity controls, recording of security relevant events, and security breach alarms; and
- establishing data and database administration policies and procedures, including clarifying personnel responsibilities, audit checks of data and system integrity, database recovery and back-up procedures.

Operations Security

This area relates to the operation of an information system, connecting the use of paper, hardware, software, databases, and networks and should include:

- establishing policies and procedures for authorization and authentication of all system users, including provisions for security of the authentication records;
- establishing policies and procedures for ensuring accuracy of data input to the system, including specification of accountabilities of personnel involved in data entry;
- procedures for detection and surveillance of system processing, including error logs, detection of record removal and security incident reporting;
- establishing contingency plans for loss of processing capability form destruction of a diskette to complete loss of a facility, including off-site storage of backup copies of essential information and software;
- maintaining an inventory of health information assets; and
- establishing formal change control procedures for any change to the information system hardware, software, database or communications network.

Security in Contracting

This part of the policy relates to the protective arrangements applying to health information in the custody of contractors but under the control of the custodian. This may include health information that is collected, compiled, used, disclosed or disposed of by a contractor.

The policy should stipulate that its provisions apply to persons working under contract to a custodian who are required to handle health information or have access to information systems or facilities where such information is handled or stored. The extent of physical, technical and personnel security requirements that a contractor will have to meet will have to be decided on a contract-by-contract basis.

Overall, the information security policy needs to meet the requirements of the duty to protect health information in **section 60** of the *Act* and the requirements of **section 8** of the Health Information Regulation, dealing with security of health information.

CHAPTER 12

CONSEQUENTIAL AMENDMENTS

12.1 OVERVIEW OF CHAPTER TWELVE

This Chapter will cover:

- an introduction to paramountcy as it applies to the *Health Information Act;*
- relationship to the *FOIP Act*;
- confidentiality provisions in other statutes that are now governed by the *Health Information Act*;
- statutory provisions that prevail over the *Health Information Act*;
- statutory provisions that maintain the status quo; and
- housekeeping amendments.

The full text of the *Health Information Act* consequential amendments and the provisions of each of the other acts that were amended consequentially are set out in the Appendix at the end of this Chapter.

12.2 INTRODUCTION TO PARAMOUNTCY AS IT APPLIES TO THE *HEALTH INFORMATION ACT*

The issue of paramountcy arises in cases where there is a conflict between a provision of the *Health Information Act* and a provision in other legislation. In these cases, the *Health Information Act* is paramount over other legislation unless specific provision is made in the *Health Information Act*, in the Health Information Regulation or in another act to make that other act or regulation paramount over the *Health Information Act*.

Section 4 of the *Health Information Act says* that if a provision of that *Act* is inconsistent or in conflict with a provision of another act or of a regulation, the provision in the *Health Information Act* prevails unless another act, or a regulation under the *Health Information Act* expressly provides that the other act or regulation, or a provision of it, prevails despite the *Health Information Act*.

A conflict or inconsistency may occur when access to information is more restricted in another act or regulation than it would be under the *Health Information Act*. For example, a provision of the *Human Tissue Gift Act* precludes the disclosure of information that could identify the donor or recipient of an organ. The secrecy provision in the *Human Tissue Gift Act* prevails over the *Health Information Act*.

A conflict or inconsistency may also occur when confidentiality provisions in the *Health Information Act* are more restrictive than in other legislation. A provision in the *Child Welfare Act* that enables records of hospital boards to be produced when they relate to court proceedings regarding a child, prevails over the *Health Information Act*.

The authority to enact regulations under the *Health Information Act* to establish that other legislation prevails or is paramount, is provided in **section 108(1)(c)**. Under that section, the Lieutenant Governor in Council may make regulations expressly providing that another act or a regulation, or a provision of it, prevails despite the *Health Information Act* for the purposes of **section 4** of the *Act*.

Under **section 4** of the Health Information Regulation, **section 3** of the *Child Welfare Act* prevails over the *Health Information Act*. Under **section 3(1)** of the *Child Welfare Act*, any person who believes, on reasonable and probable grounds, that a child is in need of protective services, must report the matter to the Director of Child Welfare. This subsection applies notwithstanding the information upon which the belief is founded is confidential and its disclosure would be prohibited under any other act.

The *Health Information Act* makes consequential amendments to fifteen different statutes. The consequential amendments are found in **sections 110 to 124** of the *Health Information Act*.

12.3 RELATIONSHIP WITH THE *FOIP ACT*

The consequential amendments in **subsection 114** of the *Health Information Act* make a number of changes to the *Freedom of Information and Protection of Privacy Act*. The definition of **"health care body"** in the previous **subsection 1(1)(g)(i)** of the *Freedom of Information and Protection of Privacy Act* is repealed and the new provision includes the Alberta Cancer Board in the definition. The amendment to **subsection 1(1)(g)(iii.1)** adds the words, 'continued under the *Cancer Programs Act*'. The definition of 'record' in **subsection 1(1)(q)** is expanded to include 'notes, images, audiovisual recordings and x-rays'.

A new **subsection 4(1)(p)** is added to the *Freedom of Information and Protection of Privacy Act*. This provision says that the *Freedom of Information and Protection of Privacy Act* does not apply to records in the custody or under the control of a public body that is a custodian of health information as defined in the *Health Information Act*. This effectively carves "health information" out of the *FOIP Act*.

New **subsections 14.1 and 35.2** have been added to the *Freedom of Information and Protection of Privacy Act*. These provisions are 'deeming' provisions. This means that when an access request or a request for correction or amendment of information is made under the *Freedom of Information and Protection of Privacy Act*, the part of the request that relates to the health information is deemed to be a request under the *Health Information Act*..

These subsections only apply if the custodian that receives the request is also a public body under the *FOIP Act* (i.e. the Minister and department, a regional health authority, the Alberta Cancer Board and the Alberta Mental Health Board) **(subsections 14.1(2) and 35.2(2)).**

12.4 CONFIDENTIALITY PROVISIONS IN OTHER STATUTES NOW GOVERNED BY THE *HEALTH INFORMATION ACT*

HOSPITALS ACT

The consequential amendments in **subsection 117** of the *Health Information Act make* a number of changes to **section 40** of the *Hospitals Act*, which is the confidentiality section of that *Act*. New **subsection 40(1.1)** of the *Hospitals Act* says that except as permitted or required under the *Hospitals Act*, health information from hospital records or persons having access to them may only be disclosed in accordance with the *Health Information Act*.

Subsection 40(2)(c) of the *Hospitals Act* enabled the Minister to compel 'diagnoses, charts or any patient information' and has been repealed. This provision is now redundant in view of the amendment to **subsection 40(2)(a)** and the broad definition of "record" in the *Health Information Act*.

A substantive change to the *Hospitals Act* arises with the repeal of **subsection 40(3),** which is the general confidentiality clause and **subsection 40(4)**, which is the offence and penalty clause. **Subsections 40(4.1), 40(5), 40(6), 40(6.1)** and **40(9)** are amended to omit reference to **subsection 40(3)**, which has been repealed.

Subsections 40(5)(a) and (a.1) of the *Hospitals Act* have been repealed. **Subsection 40(5)(a)** provided authority to disclose to the patient or legal representative and **subsection 40(5)(a.1)** provided authority to disclose in accordance with consent or in the best interests of the individual. Provisions governing these disclosures are now found in **sections 34 and 35** of the *Health Information Act*.

Subsection 40(5)(b) of the *Hospitals Act* is repealed. **Subsection 40(5)(b)** provided authority to disclose to the Director of Medical Services under the *Occupational Health and Safety Act*. Authority for this disclosure is addressed under **section 40(6)(a)(i)** of the *Hospitals Act*.

Subsections 40(5.1) and 40(7) of the *Hospitals Act* have been repealed. **Subsection 40(5.1)** provided authority to disclose hospital records pursuant to a subpoena under the *Child Welfare Act*. **Subsection 40(7)** provided authority to disclose hospital records to a medical examiner pursuant to the *Fatality Inquiries Act*. These disclosures are addressed in the respective consequential amendments in the *Health Information Act* to **section 75(3)** of the *Child Welfare Act* and **section 22(3)** of the *Fatality Inquiries Act*.

Subsections 40(6)(b), (c.1) and (d.1) of the *Hospitals Act* are repealed. **Subsection 40(6)(b)** provided authority to disclose for purposes of research, medical review and training, **subsection 40(6)(c.1)** provided authority to disclose for purposes of patient transfer between hospitals and nursing homes, and **subsection 40(6)(d.1)** provided authority to disclose in accordance with the *Radiation Protection Act*. Provisions governing these or similar disclosures are now under **section 35** of the *Health Information Act*.

Subsections 40(10) to (12) of the *Hospitals Act* have been repealed. These subsections created the remedy of a court application for individuals that were refused access to their own health records. A different remedy is now provided in the *Health Information Act*. Under **section 73** of the *Health Information Act*, applicants who are refused access to their own health information may request that the Commissioner review the custodian's decision to deny access to the information.

Subsection 40(13)(a.1) has been added and says that the definition of "health information" is as defined in the *Health Information Act*.

MENTAL HEALTH ACT

The consequential amendments in **subsection 119** of the *Health Information Act* make a number of changes to **section 17** of the *Mental Health Act*, which is the confidentiality section of that *Act*.

Subsection 17(1)(b.1) has been added and says that the definition of "health information" is as defined in the *Health Information Act*.

New **subsection 17(1.1)** of the *Mental Health Act* says that except as permitted or required under the *Mental Health Act*, health information from a diagnostic and treatment center or persons having access to them may only be disclosed in accordance with the *Health Information Act* (either under **Part 2 (Individual's Right to Access Individual's Health Information)** or **Part 5 (Disclosure of Health Information)**).

Subsection 17(3)(c) of the *Mental Health Act* enabled the Minister to compel 'diagnoses, charts or any patient information' and is repealed. This provision is now redundant in view of the broad definition of "records" in the *Health Information Act.*

A substantive change to the *Mental Health Act* arises as **subsection 17(4)**, which is the general confidentiality clause and **subsection 17(5)**, which is the offence and penalty clause, are repealed. **Subsections 17(5.1) and 17(6)** of the *Mental Health Act* are amended to omit reference to **subsection 17(4)**, which has been repealed.

Subsections 17(6)(a) and (b) of the *Mental Health Act* are repealed. **Subsection 17(6)(a)** provided authority to disclose to the patient or legal representative and **subsection 17(6)(b)** provided authority to disclose in accordance with consent or in the best interests of the individual. Provisions governing these disclosures are now under **sections 34 and 35** of the *Health Information Act*.

Subsections 17(6)(c) and (o) of the *Mental Health Act* are repealed. **Subsection 17(6)(c)** provided authority to disclose to a department or agency of the government or to a physician if that entity was responsible for providing continued treatment and care. **Subsection 17(6)(o)** provided authority to disclose for purposes of transferring responsibility for patient care purposes amongst boards and regional health authorities. Authority for these disclosures is now provided in **section 35** of the *Health Information Act*.

Subsections 17(6)(g) and (k) of the *Mental Health Act* are repealed. **Subsection 17(6)(g)** provided authority to disclose for purposes of research and medical review and **subsection 17(6)(k)** provided authority to disclose for purposes of training. Provisions governing these or similar disclosures are now under **section 35** of the *Health Information Act*.

Subsections 17(7) and 17(9) of the *Mental Health Act* are repealed. **Subsection 17(7)** provided authority to disclose records pursuant to a subpoena under the *Child Welfare Act*. **Subsection 17(9)** provided authority to disclose records to a medical examiner pursuant to the *Fatality Inquiries Act*. These disclosures are addressed in the respective consequential amendments in the *Health Information Act* to **section 75(3)** of the *Child Welfare Act* and **section 22(3)** of the *Fatality Inquiries Act*.

Subsections 17(10) to **(12)** of the *Mental Health Act* are repealed. These subsections created the remedy of a court application for individuals that were refused access to their own health records. A different remedy is now provided in the *Health Information Act*.

NURSING HOMES ACT

The consequential amendment in **section 120** of the *Health Information Act* is the addition of **subsection 27(4)** to the *Nursing Homes Act*. **Subsection 27(4)** says that **subsection 27(2)** of the *Nursing Homes Act* does not apply to health information within the meaning of the *Health Information Act*.

Subsection 27(2) of the *Nursing Homes Act* was the general confidentiality provision that applied to information in resident's records. This amendment means that health information located in resident's records will be governed by the *Health Information Act* rather than by the *Nursing Homes Act*.

REGIONAL HEALTH AUTHORITIES ACT

The consequential amendment in **section 124** of the *Health Information Act* repeals **subsection 21(1)(o)** of the *Regional Health Authorities Act*. This subsection provided authority for the Lieutenant Governor in council to make regulations about confidentiality requirements for information obtained in the administration of the *Regional Health Authorities Act* or in providing health services or health related services under that *Act*.

12.5 STATUTORY PROVISIONS THAT PREVAIL OVER THE *HEALTH INFORMATION ACT*

ALBERTA HEALTH CARE INSURANCE ACT

The consequential amendments in **subsection 110(2)** of the *Health Information Act* make a number of changes to **section 13** of the *Alberta Health Care Insurance Act*, which is the secrecy of information section of that *Act*. The former **subsection 13(1)** of the *Alberta Health Care Insurance Act* is repealed. The new **subsection 13(1)** says that except as permitted or required under the *Alberta Health Care Insurance Act*, health information may only be disclosed in accordance with the *Health Information Act* **(Part 5 – Disclosure of Health Information)**.

The **new section 13(1.01)** says that **subsections 13(3.2) and 13(4)** of the *Health Care Insurance Act* prevail over the *Health Information Act* if there is an inconsistency or conflict between **subsections 13(3.2) or 13(4)** and the *Health Information Act*. The words, 'or communicate' follow the words, 'disclose' in the previous provisions in **subsections 13(2)(2.1) and (3)** of the *Alberta Health Care Insurance Act*. The words 'or communicate' are redundant and have been deleted in the revisions to **subsections 13(2)(2.1) and (3)**.

New subsection 13(3.2) of the *Alberta Health Care Insurance Act* says that the Minister may disclose identifying health information to the individual who is the subject of the information, to a person acting on behalf of the individual or to a person in accordance with the consent of the individual. **Subsections 13(4)(e), (e.1) and (e.2)** are repealed, as the new **subsection 13(3.2)** covers these situations.

CANCER PROGRAMS ACT

The consequential amendment in **section 111** of the *Health Information Act* adds **section 20.11** to the *Cancer Programs Act*. **Section 20.11** says that **Part 1.1** of *the Cancer Programs Act* prevails over the *Health Information Act* if there is an inconsistency or conflict between that part and the *Health Information Act*. **Part 1.1** governs the cancer registry established by the *Cancer Programs Act*.

Physicians and laboratories must report all reportable cancers and any additional information required by the regulations under the *Cancer Programs Act* to the Alberta Cancer Board for the cancer registry. The cancer registry also contains information obtained under the *Alberta Health Care Insurance Act*, from a hospital under the *Hospitals Act*, from the Alberta Cancer Board's hospitals and out-patient clinics and programs, and from any other source specified by the Minister. The authorized uses and disclosures of the information collected by the cancer registry are as described in the *Cancer Programs Act* and regulations. For example, this information may be used and disclosed for research.

CHILD WELFARE ACT

The consequential amendment in **section 112(1)** of the *Health Information Act* to **section 75(3)** of the *Child Welfare Act* maintains the paramountcy of the *Child Welfare Act* for records that are subpoenaed and otherwise confidential under other legislation such as the *Health Information Act* and the *Public Health Act*.

In the past, **section 75(3)** of the *Child Welfare Act* established the paramountcy of the *Child Welfare Act* over confidentiality provisions in legislation such as the *Hospitals Act*, the *Mental Health Act* and the *Public Health Act* for subpoenas issued in child welfare proceedings. This provision enabled the court to issue subpoenas that required entities including a board under the *Hospitals Act* and the *Mental Health Act* to produce records that relate to court proceedings regarding a child.

HUMAN TISSUE GIFT ACT

The consequential amendment in **section 118** of the *Health Information Act* is the addition of **section 11 (3)** to the *Human Tissue Gift Act*. This new provision establishes the paramountcy of **subsection 11(1)** of the *Human Tissue Gift Act* over the *Health Information Act* if the two Acts are inconsistent or in conflict. **Subsection 11(1)** of the *Human Tissue Gift Act* precludes the disclosure of information that could identify the donor or recipient of an organ.

PUBLIC HEALTH ACT

The consequential amendment in **section 123(2)** of the *Health Information Act* repeals **subsection 63(4)(d)** of the *Public Health Act*, which authorized disclosure to a person conducting research or medical review if the disclosure ensured confidentiality of the information.

The consequential amendment in **section 123(3)** of the *Health Information Act* repeals **section 83** of the *Public Health Act*, which was the earlier paramountcy provision in this legislation. A **new section 83** is substituted in the *Public Health Act*, which says that except for the *Alberta Bill of Rights*, the *Public Health Act* prevails over any enactment that it conflicts with or is inconsistent with, including the *Health Information Act*. This amendment retains the paramountcy of the *Public Health Act* over other legislation.

12.6 STATUTORY PROVISIONS THAT MAINTAIN THE STATUS QUO

FATALITY INQUIRIES ACT

The consequential amendment in **section 113(2)** of the *Health Information Act* to **section 22(3)** of the *Fatality Inquiries Act* retains the ability of a medical examiner or investigator to inspect and make copies of diagnostic and treatment records of individuals for services received under the *Mental Health Act* or the *Hospitals Act*.

The consequential amendment in **section 113(3)** of the *Health Information Act* to **section 40(1.1)** of the *Fatality Inquiries Act* enables a judge to admit any relevant part of a record in evidence to make findings and recommendations and a report, notwithstanding any other Act, regulation or other law. The consequential amendment no longer includes specific reference to records under the *Mental Health Act* and the *Hospitals Act* in this provision.

HEALTH FACILITIES REVIEW COMMITTEE ACT

The consequential amendment in **section 115** of the *Health Information Act* to **section 10 (2)(b)** of the *Health Facilities Review Committee Act* maintains the status quo under the earlier legislation. The Alberta Health Facilities Review Committee is not entitled to inspect hospital records containing individually identifying health information within the meaning of the *Health Information Act*, except with the consent of the individual or the individual's guardian.

HEALTH PROFESSIONS ACT

The consequential amendment in **section 116** of the *Health Information Act* to **section 155(4)** of the *Health Professions Act* maintains the status quo under the earlier legislation. **Section 155(4)** of the *Health Professions Act* is a consequential amendment to **section 17(6)** of the *Mental Health Act* that allows health information to be disclosed to a hearings director of a college under the *Health Professions Act* if in compliance with a notice under that Act.

PROTECTION FOR PERSONS IN CARE ACT

The consequential amendment in **section 122** of the *Health Information Act* to **section 7(5)(b)** of the *Protection for Persons in Care Act* maintains the status quo under the earlier legislation. An investigator is not entitled to inspect or copy an agency's health information records of a person within the meaning of the *Health Information Act*, except with consent of the person or the person's guardian.

12.7 HOUSEKEEPING AMENDMENTS

ALBERTA HEALTH CARE INSURANCE ACT

Subsections 13(5) to (5.4) of the *Alberta Health Care Insurance Act* have been repealed. **Subsection 13(5)** would be redundant as this authorizes the Minister to disclose information in statistical form. **Subsections 13(5.1) to (5.4)** provided for disclosure for research purposes, which is now covered under the *Health Information Act*. **New subsection 13(12)** defines the terms "health information" and "individually identifying" in the *Alberta Health Care*

Insurance Act, for consistency with the *Health Information Act*.

The words, "residents' or" are deleted from **subsections 13(5.5) and (5.6)**. This provision previously enabled the Minister to enter into agreements for the disclosure of residents' or practitioners' registration information. The authority of the Minister to enter into agreements for disclosure of individually identifying information is now covered under **section 39** of the *Health Information Act*.

Some housekeeping changes were made to **section 14** of the *Alberta Health Care Insurance Act*, which is the protection from action provision, in the consequential amendments made in **subsection 110(3)** of the *Health Information Act*. The former words, 'furnishes' and 'furnishing' in **section 14** are changed to read 'discloses' and 'disclosure', so the new words are consistent with the language in the *Health Information Act*. A similar change is made in the revision to **subsection 13(4)**, before **clause (a)**. Similarly, the former words, 'provide' and 'provided' in **section 13(4.1)** have been changed to read 'disclose' and 'disclosed'.

FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT

The amendments to **subsections 76(2) and 77(7)** of the *Freedom of Information and Protection of Privacy Act* are housekeeping matters, as the meaning of these provisions is not changed. The amendment to **subsection 86(1)(e)** of the *Freedom of Information and Protection of Privacy Act* expands the scope of this offence provision so that it is the same as in the *Health Information Act*. The previous **subsection 86(1)(e)** precluded a person from willfully destroying records subject to that *Act* with the intent to evade an access request. In the amendment to **subsection 86(1)(e)**, it is also an offence to direct another person to willfully destroy records to avoid an access request.

HOSPITALS ACT

Housekeeping amendments are made to **subsections 40(2)(a) and (b)**, which change the word 'medical' to 'health information', so the language is consistent with the *Health Information Act*. Similarly, **subsection 40(5)(c)** is amended by changing the words, 'divulge any diagnosis, record or' to 'disclose health'. Changing the word 'divulge' to 'disclose' amends **subsections 40(6)(g) and (h)**.

MENTAL HEALTH ACT

A housekeeping amendment is made to **subsection 17(3)(a)** of the *Mental Health Act*, which changes the word 'medical' to 'health information', so the language is consistent with the *Health Information Act*. Changing the words, 'diagnosis, record or' to 'health' amends **subsection 17(6)**.

PHARMACY AND DRUG ACT

The consequential amendment in **section 121** of the *Health Information Act* is a housekeeping amendment involving the addition of a new section **47.1** to the *Pharmacy and Drug Act*. **Section 47.1** amends four definitions in **subsection 1(1)** of the *Health Information Act* to refer to the *Pharmacy and Drug Act* rather than the *Pharmaceutical Profession Act*.

APPENDIX TO CHAPTER 12

This Appendix contains the full text of the consequential amendment made to the *Health Information Act* and the provision of the other *Act* that was amended consequentially.

1. Alberta Health Care Insurance Act - Amends R.S.A. 1980 c. A-24

A. Health Information Act Provision

110(1) The *Alberta Health Care Insurance Act* is amended by this section.

(2) Section 13 is amended

(a) by repealing subsection (1) and substituting the following:

> 13(1) Except as permitted or required under this Act, the Minister or a person employed in the administration of this Act and authorized by the Minister may disclose health information acquired under this Act or the *Health Insurance Premiums Act* only in accordance with the *Health Information Act*.
>
> (1.01) If there is an inconsistency or conflict between subsection (3.2) or (4) and the *Health Information Act*, subsection (3.2) or (4), as the case may be, prevails.

(b) in subsections (2), (2.1) and (3) by striking out "or communicate";

(c) by adding the following after subsection (3.1):

> (3.2) The Minister or a person employed in the administration of this Act and authorized by the Minister may disclose individually identifying health information, other than a diagnosis given by a person who has provided health services, acquired under this Act
>
> (a) to the individual who is the subject of the information,
>
> (b) to a person referred to in section 104(1)(c) to (i) of the *Health Information Act* who is acting on behalf of the individual who is the subject of the information, or
>
> (c) to a person other than the individual who is the subject of the information if the individual has consented to the disclosure in accordance with section 34 of the *Health Information Act*.

(d) in subsection (4)

(i) by striking out the words preceding clause (a) and substituting the following:

(4) The Minister or a person employed in the administration of this Act and authorized by the Minister may disclose information pertaining to the date on which health services were provided and a description of those services, the name and address of the person who provided the services, the registration number of the person who received the services, the benefits paid for those services and the person to whom they were paid, but the information may be disclosed only

(ii) by repealing clauses (e), (e.1) and (e.2);

(e) in subsection (4.1)

(i) by striking out "provide" and substituting "disclose";

(ii) by striking out "provided" and substituting "disclosed";

(f) by repealing subsections (5) to (5.4);

(g) in subsections (5.5) and (5.6) by striking out "residents' or";

(h) by adding the following after subsection (11):

(12) In this section,

(a) "health information" means health information as defined in the *Health Information Act*;

(b) "individually identifying", when used to describe health information, means that the identity of the individual who is the subject of the information can be readily ascertained from the information.

(3) Section 14 is amended

(a) by striking out "furnishes" and substituting "discloses";

(b) by striking out "furnishing" and substituting "disclosure".

B. Alberta Health Care Insurance Act Provision

13(1) The Minister and every person employed in the administration of this Act or the Health Insurance Premiums Act shall preserve secrecy with respect to all matters that come to his knowledge in the course of his employment and shall not communicate any of those matters to any other person except as otherwise provided in this section.

(2) The Minister or a person employed in the administration of this Act and authorized by the Minister may disclose or communicate information pertaining to the date on which health services were provided, a description of those services, any diagnosis given by a person who provided the services, the name and address of the person who provided the services, the benefits paid for those services and the person to whom they were paid, the name and address of the person to whom the services were provided and any other information pertaining to the nature of the health services provided

(a) repealed 1986 c3 s6,

(b) to any committee established to advise the Minister in respect of matters under section 8.

(2.1) The Minister or a person employed in the administration of this Act and authorized by the Minister may, in connection with the administration of the *Criminal Code (Canada)*, disclose or communicate to the Minister of Justice and Attorney General, or a person designated by him, information pertaining to the date on which health services were provided, a description of those services, any diagnosis given by a person who provided the services, the name and address of the person who provided the services, the benefits paid for those services and the person to whom they were paid, the name and address of the person to whom the services were provided and any other information coming to the knowledge of any person employed in the administration of this Act in the course of his employment.

(3) The Minister or a person employed in the administration of this Act authorized by the Minister may disclose or communicate information pertaining to the date on which health services were provided and a description of those services, the name and address of the person who provided the services, the benefits paid for those services and the person to whom they were paid, the name and address of the person to whom the services were provided and any other information pertaining to the nature of the health services provided, to the Alberta Cancer Board, The Workers' Compensation Board, a director under the *Child Welfare Act*, the Sexually Transmitted Disease Control Unit of the Department of Health, or the Director of Medical Services appointed under the *Occupational Health and Safety Act*, if

(a) a member or officers of the Board, a director under the *Child Welfare Act*, or an officer of the Unit, or the Director of Medical Services, as the case may be, makes a written request for it, and

(b) the information required is necessary and relevant to a matter being dealt with by the Board, a director under the *Child Welfare Act*, an officer of the Unit or the Director of Medical Services.

(4) The Minister or a person employed in the administration of this Act authorized by the Minister may furnish information pertaining to the date on which health services were provided and a description of those services, the name and address of the person who provided the services, the registration number of the person who received the services, the benefits paid for those services and the person to whom they were paid, but the information may be furnished only

(e) to the resident or his dependant who received the services or to any other person with the written consent of the resident or dependant who received the services,

(e.1) to the solicitor, personal representative, guardian or other legal representative of the resident or dependant referred to in clause (e), or to the committee or guardian of his estate,

(e.2) if the information relates to a personal decision made or to be made under the *Personal Directives Act*, to any person who is authorized by that Act to make the decision and to the Court that is considering the decision in accordance with that Act,

(4.1) The Minister or a person employed in the administration of this Act and authorized by the Minister may provide information, other than information related to health services, about a person, but the information may only be provided in connection with the administration of the *Seniors Benefit Act*.

(5) Information in the hands of the Minister may be published by the Minister or the Government in statistical form if the individual names of persons are not thereby revealed or made identifiable.

(5.1) The Minister or a person authorized by the Minister may disclose, for the purpose of bona fide health related research, any information obtained under this Act or the *Health Insurance Premiums Act* other than

(a) the names of individuals to whom the information relates, or

(b) information that would enable the person who is conducting the research to identify the names of those individuals.

(5.2) The Minister or a person authorized by the Minister may disclose, for the purpose of bona fide health related research, any information obtained under this Act or the *Health Insurance Premiums Act*, including the names of individuals to whom the information relates, if the Minister or authorized person is satisfied that the person conducting the research will not reveal or make identifiable the name of any individual to whom the information relates without the consent of the individual.

(5.3) A person who receives information under subsection (5.2) and reveals or makes identifiable the name of an individual to whom the information relates without the consent of the individual is guilty of an offence and liable to a fine of not more than $10 000.

(5.4) A person who receives information under subsection (5.2) (in this section referred to as "the researcher") shall not contact an individual to whom the information relates unless

(a) the researcher provides the Minister with the reasons for wanting to contact the individual,

(b) the Minister or a person authorized by the Minister is satisfied that the contact is appropriate and is for the purpose of bona fide health related research,

(c) the Minister or authorized person contacts the individual to determine whether the individual consents to being contacted by the researcher, and

(d) the individual consents.

(5.5) The Minister may enter into an agreement respecting the disclosure of residents' or practitioners' registration information obtained under this Act or the *Health Insurance Premiums Act* with

(a) any Minister or government, or

(b) a person or entity designated in the regulations.

(5.6) The Minister may, in accordance with an agreement made under subsection (5.5), disclose residents' or practitioners' registration information obtained under this Act or the *Health Insurance Premiums Act*.

14 If a practitioner or an agent or employee of a practitioner furnishes information to the Minister or to a person employed in the administration of this Act, no action lies against the practitioner or the agent or employee in respect of the furnishing of that information.

2. Cancer Programs Act - Amends R.S.A. 1980 c. C-1

A. Health Information Act Provisions

111(1) The *Cancer Programs Act* is amended by this section.

(2) The following is added after section 20.1:

> 20.11 If there is an inconsistency or conflict between this Part and the *Health Information Act*, this Part prevails.

B. Cancer Programs Act Provisions

PART 1.1 CANCER REGISTRY

20.1 In this Part, "reportable cancer" means a cancer specified by the regulations as a reportable cancer.

20.2(1) The board shall, subject to the regulations, establish a cancer registry.

(2) The cancer registry must contain the information respecting reportable cancers obtained under section 20.5.

(3) The cancer registry may, subject to any directions specified in the regulations, contain information

(a) obtained under section 13(3) of the Alberta Health Care Insurance Act

(b) obtained under the Hospitals Act from a hospital that is not a provincial cancer hospital,

(c) obtained from the board's hospitals, out-patient clinics and programs, and (d) obtained from any other source specified by the Minister.

20.3(1) The information in the cancer registry is private and confidential.

(2) Section 40 of the Hospitals Act does not apply to information in the cancer registry.
20.4 The information in the cancer registry is to be used for the following purposes:

(a) to assess and improve the standards of treatment and care provided to cancer patients;

(b) to assist in the treatment and care of the person who is the subject of the information;

(c) to assist in cancer research, education and prevention;

(d) to compile statistics on cancer;

(e) any other purpose specified by the Minister.

20.5(1) A physician who knows or has reason to believe that a patient under the physician's care or supervision has a reportable cancer shall, as soon as practicable, provide the board with the information prescribed by the regulations.

(2) A person who is responsible for a laboratory in which an examination of a specimen from a human body is conducted that reveals a reportable cancer shall, as soon as practicable, provide the board with the information prescribed by the regulations.

(3) After receiving information under subsection (1) or (2), the board may request the physician or person responsible for the laboratory to provide any additional information that the board considers necessary respecting the reportable cancer, the person who has cancer or the examination.

(4) No action or other proceeding for damages lies against a physician or person responsible for a laboratory for providing information to the board under this section.

F5

20.6(1) The Minister or the board with the approval of the Minister may enter into an agreement with the Government of Canada or the government of a province or with any person that relates to the disclosure of information in the cancer registry.

(2) An agreement under subsection (1) shall require that the information disclosed remain confidential.

20.7(1) The board may use the information in the cancer registry for the purposes referred to in section 20.4.

(2) The board shall disclose the information in the cancer registry

(a) to the Minister in the manner and form specified by the Minister,

(b) to any person specified by the Minister where the Minister believes it is in the public interest that the information be disclosed to that person, and

(c) to any person when required by law.

(3) The board may disclose the information in the cancer registry

(a) to the person who is the subject of the information or to that person's designate or legal representative;

(b) in statistical form if the person who is the subject of the information is not revealed or made identifiable;

(c) to a person conducting bona fide research or a medical review if the disclosure is made in a manner that ensures the confidentiality of the information;

(d) to a person authorized to receive the information under an agreement referred to in section 20.6; (e) to a person or class of persons authorized to receive the information by the regulations.

20.8(1) No person shall disclose information in the cancer registry to a person unless disclosure of information to that person is authorized under section.

20.8(2) No person shall review or examine the information in the cancer registry unless disclosure of the information to that person is authorized under section.

20.8(3) A person who contravenes subsection (1) or (2) is guilty of an offence and is liable to a fine of not more than $10 000.

20.9 The Minister may make regulations

(a) prescribing a list of cancers or adopting a published list of cancers in whole or in part as reportable cancers;

(b) respecting the information to be provided to the board under section 20.5;

(c) respecting the establishment and operation of the cancer registry, including regulations requiring the board to enter certain information in the cancer registry;

(d) authorizing the board to disclose information in the cancer registry to a person or class of persons.

3. Child Welfare Act - Amends S.A. 1984 c. C-8.1

A. Health Information Act Provision

112(1) The *Child Welfare Act* is amended by this section.

(2) Section 75(3) is amended by striking out "*the Hospitals Act, the Mental Health Act*" and substituting "the *Health Information Act*".

B. Child Welfare Act Provision

75(1) Notwithstanding Part XIX of the *Criminal Code (Canada),* the Court may issue a subpoena requiring

(a) the Commission under the *Alcohol and Drug Abuse Act,*
(b) a board under the *Hospitals Act,*
(c) a board under the *Mental Health Act,* or
(d) the Director under the *Public Health Act,*
(e) repealed 1990 c29 s3,

or his designate to produce any documents, records or other information he has in his possession or under his control that may relate to the proceedings before the Court with respect to a child.

(3) If, as the result of the issuing of a subpoena under subsection (1), a person is required to produce any documents, records or other information that is otherwise confidential under the *Alcohol and Drug Abuse Act*, the *Hospitals Act*, the *Mental Health Act* or the *Public Health Act*, as the case may be, the documents, records or other information shall be dealt with in accordance with this section.

4. Fatality Inquiries Act – Amends R.S.A. 1980 c. F-6

A. Health Information Act Provision

113(1) The *Fatality Inquiries Act* is amended by this section.

(2) Section 22(3) is repealed and the following is substituted:

> (3) Notwithstanding any other Act, regulation or other law, a medical examiner is entitled to inspect and make copies of any diagnosis, record or information relating to
>
> (a) a person receiving diagnostic and treatment services in a diagnostic and treatment centre under the *Mental Health Act*, or
>
> (b) a patient under the *Hospitals Act*.

(3) Section 40(1.1) is amended by striking out "section 17(4) of the *Mental Health Act* or section 40(3) of the *Hospitals Act* or".

B. Fatality Inquiries Act Provision

22(3) Notwithstanding section 17(4) of the *Mental Health Act* or section 40(3) of the *Hospitals Act* or any other Act, regulation or other law, a medical examiner is entitled to inspect and make copies of any diagnosis, record or information relating to a person receiving diagnostic and treatment services in a centre as provided in section 17(9) of the *Mental Health Act* and to inspect and make copies of any diagnosis, record or information relating to a patient as provided in section 40(7) of the *Hospitals Act*.

40(1.1) Notwithstanding section 17(4) of the *Mental Health Act* or section 40(3) of the *Hospitals Act* or any other Act, regulation or other law, a judge may admit in evidence all or any relevant part of a diagnosis, record or information referred to in section 22(3) to enable him to make findings and recommendations and to report in respect of any or all of the matters set out in section 47.

5. Freedom of Information and Protection of Privacy Act - Amends S.A. 1994 c. F-18.5

A. Health Information Act Provision

114(1) The *Freedom of Information and Protection of Privacy Act* is amended by this section.

(2) Section 1(1) is amended

> (a) in clause (g)
>
> > (i) by repealing subclause (i) and substituting the following:

(i) the board of an approved hospital as defined in the *Hospitals Act* other than an approved hospital that is

(A) owned or operated by a regional health authority under the *Regional Health Authorities Act*, or

(B) established and operated by the Alberta Cancer Board continued under the *Cancer Programs Act*,

(ii) in subclause (iii.1) by adding "continued under the *Cancer Programs Act*" after "Board";

(b) in clause (q) by adding "notes, images, audiovisual recordings, x-rays," before "books".

(3) Section 4(1) is amended by adding the following after clause (o):

(p) health information as defined in the *Health Information Act* that is in the custody or under the control of a public body that is a custodian as defined in the Health Information Act.

(4) The following is added after section 14:

14.1(1) If a request is made under section 7(1) for access to a record that contains information to which the *Health Information Act* applies, the part of the request that relates to that information is deemed to be a request under section 8(1) of the *Health Information Act* and that Act applies as if the request had been made under section 8(1) of that Act.

(2) Subsection (1) does not apply if the public body that receives the request is not a custodian as defined in the *Health Information Act*.

(5) The following is added after section 35.1:

35.2(1) If a request is made under section 35(1) to correct personal information that contains information to which the *Health Information Act* applies, the part of the request that relates to that information is deemed to be a request under section 13(1) of the *Health Information Act* and that Act applies as if the request had been made under section 13(1) of that Act.

(2) Subsection (1) does not apply if the public body that receives the request is not a custodian as defined in the *Health Information Act*.

(6) Section 76(2) is amended by striking out "section 68(1), (2), (3)(a) to (d), (4) and (5)" and substituting "section 68(1) to (5)".

(7) Section 77(7) is amended by striking out "68(1), (2), (3)(a) to (d), (4) and (5)" and substituting "68(1) to (5)".

(8) Section 86(1)(e) is amended by adding ", or direct another person to do so," after "Act".

B. Freedom of Information and Protection of Privacy Act Provision

1(1) In this Act,

(g) "health care body" means

(i) the board of an approved hospital as defined in the *Hospitals Act* other than an approved hospital that is owned and operated by a regional health authority under the *Regional Health Authorities Act*,

(iii.1) the Alberta Cancer Board,

(q) "record" means a record of information in any form and includes books, documents, maps, drawings, photographs, letters, vouchers and papers and any other information that is written, photographed, recorded or stored in any manner, but does not include software or any mechanism that produces records;

4(1) This Act applies to all records in the custody or under the control of a public body, including court administration records, but does not apply to the following:

76(2) On completing an inquiry, an adjudicator has the same duty to dispose of the issues, the same power to make orders and the same duty to notify others of those orders as the Commissioner has under section 68(1), (2), (3)(a) to (d), (4) and (5).

77(7) In carrying out an investigation and review under this section, the Commissioner has all of the powers and duties set out in sections 54, 57,65, 66 and 68(1), (2), (3)(a) to (d), (4) and (5), and sections 55, 56, 58 and 60 apply.

86(1) A person must not willfully

(f) destroy any records subject to this Act with the intent to evade a request for access to the records.

6. Health Facilities Review Committee Act – Amends R.S.A. 1980 c. H-4

A. Health Information Act Provision

115(1) The *Health Facilities Review Committee Act* is amended by this section.

(2) Section 10(2)(b) is repealed and the following is substituted:

> (b) records containing individually identifying health information within the meaning of the *Health Information Act* unless the patient or the patient's guardian consents to those records being inspected.

B. Health Facilities Review Committee Act Provisions

10(1) The Committee, with respect to a visit or an investigation under this Act, is entitled to access to the records of the hospital for the purpose of inspecting them, making copies of them or taking extracts from them.

(2) Subsection (1) does not apply to

a) the financial records of the hospital that relate to the operation of the hospital, or
b) the medical and clinical records of a patient unless the patient or his guardian gives his consent to those records being inspected.

7. Health Professions Act – Amends S.A. 1999 c. H-5.5

A. Health Information Act Provision

116(1) The *Health Professions Act* is amended by this section.

(2) Section 155(4) is amended by striking out "after clause (o)" and substituting "before clause (p)".

B. Health Professions Act Provision

155(4) The *Mental Health Act* is amended in section 17(6) by adding the following after clause (o):

> (o.1) to a hearings director of a college under the *Health Professions Act* if the disclosure is made in compliance with a notice under section 73 or 74 of the *Health Professions Act*,

8. Hospitals Act - Amends R.S.A. 1980 c. H-11

A. Health Information Act Provision

117(1) The *Hospitals Act* is amended by this section.

(2) Section 40 is amended

(a) by adding the following after subsection (1):

(1.1) Except as permitted or required under this Act, a board or employee of a board, the Minister or a person authorized by the Minister or a physician may disclose health information obtained from hospital records or from persons having access to them only in accordance with the *Health Information Act*.

(b) in subsection (2)

(i) in clauses (a) and (b) by striking out "medical" and substituting "health information";

(ii) by repealing clause (c);

(c) by repealing subsections (3) and (4);

(d) in subsection (4.1) by striking out "Notwithstanding subsection(3) or any other law, the Minister" and substituting "The Minister";

(e) in subsection (5)

(i) by striking out "Notwithstanding subsection (3) or any other law, a board" and substituting "A board";

(ii) by repealing clauses (a), (a.1) and (b);

(iii) in clause (c) by striking out "divulge any diagnosis, record or" and substituting "disclose health";

(f) by repealing subsection (5.1);

(g) in subsection (6)

(i) by striking out "Notwithstanding subsection (3) or any other law," and substituting "The following applies with respect to disclosing records of diagnostic and treatment services in respect of a patient:";

(iii) by repealing clauses (b), (c.1) and (d.1);

(iv) in clauses (g) and (h) by striking out "divulge" and substituting "disclose";

(h) in subsection (6.1) by striking out "Notwithstanding subsection(3) or any other law, the board" and substituting "The board";

(i) by repealing subsection (7);

(j) by repealing subsection (9) and substituting the following:

> (9) An Appeal Board is entitled, for the purpose of an appeal under section 36, to inspect and make copies of any health information or other records relating to a patient and may admit a copy of the health information or other records in evidence of the appeal, but all proceedings related to the health information or other records must be held in private.

(k) by repealing subsections (10) to (12);

(l) in subsection (13) by renumbering clause (a) as clause (a.1) and by adding the following before clause (a.1): (a) "health information" means health information as defined in the *Health Information Act*;

B. Hospitals Act Provision

40(1) The board of each approved hospital shall cause to be kept by the attending physician or any other person providing diagnostic or treatment services to a patient a record of the diagnostic and treatment services provided in respect of each patient in order to assist in providing a high standard of medical care.

(2) For the purposes of assessing the standards of care furnished to patients, improving hospital or medical procedures, compiling medical statistics, conducting medical research, enforcing the Crown's right of recovery under Part 5, or for any other purpose considered by the Minister to be in the public interest, the Minister, or a person authorized by the Minister, may require that all or any of the following be sent to him or a person designated by him:

(a) medical and other records of any patient;

(b) extracts from and copies of any medical or other records of any patient;

(c) diagnoses, charts or any information available in respect of a patient.

(3) Information obtained from hospital records or from persons having access thereto shall be treated as private and confidential information in respect of any individual patient and shall be used solely for the purposes described in subsection (2) and the information shall not be published, released or disclosed in any manner that would be detrimental to the personal interests, reputation or privacy of a patient or the patient's attending physician or any other person providing diagnostic or treatment services to a patient.

(4) A person who knowingly and willfully releases or discloses information obtained from hospital records to a person not authorized to receive the information is guilty of an offence and liable to a fine of not more than $2000.

(4.1) Notwithstanding subsection (3) or any other law, the Minister or any person authorized by the Minister may, for the purpose of enforcing the Crown's right of recovery under Part 5, disclose information obtained under subsection (2).

(5) Notwithstanding subsection (3) or any other law, a board or employee of a board, the Minister or a person authorized by the Minister, or a physician or a member of a professional staff may

(a) divulge any diagnosis, record or information to the patient to whom the diagnosis, record or information relates or to his legal representative,

> (a.1) with the written consent of a patient or his guardian or without that consent if the patient is not mentally competent and does not have a guardian, divulge any diagnosis, record or information relating to the patient to any person, if in the opinion of the person making the disclosure it is in the best interests of the patient to disclose the information,

(b) without written consent of the patient, divulge any diagnosis, record or information relating to the patient to the Director of Medical Services appointed under *the Occupational Health and Safety Act* when that information relates to an accident which occurred in respect of that patient's occupation or one or more of his former occupations or a disease which is related to that patient's occupation or one or more of his former occupations, and

(c) without written consent of a patient, divulge any diagnosis, record or information relating to the patient to

> (i) a Workers' Compensation Board,
>
> (ii) the Alberta Blue Cross Plan, or
>
> (iii) any other provincial hospital insurance authority, if the information is required in order to establish responsibility for payment by the organization or insurer, or to any other hospital to which the patient may be transferred or admitted or to other attending physicians or attending professional staff.

(5.1) Notwithstanding subsection (3) or any other law, if the Provincial Court issues a subpoena pursuant to the *Child Welfare Act*, a board, an employee of a board, a physician, a member of a professional staff, the Minister or a person authorized by the Minister shall release, in accordance with that Act, any diagnosis, record or information in respect of the child to whom the proceedings before the Provincial Court relate or with respect to a guardian of that child.

(6) Notwithstanding subsection (3) or any other law,

> (a) the Minister may, for the purposes mentioned in subsection (2) and without the consent of any other person, disclose to or obtain from

(i) the Director of Medical Services appointed under the *Occupational Health and Safety Act*,

(i.1) the Alberta Medical Association (C.M.A.-Alberta Division),

(ii) the Department of National Health and Welfare for purposes in connection with the *Canada Health Act (Canada)*, or

(iii) the government of a province of Canada or an agent of that government for purposes in connection with any health services or hospital care insurance plan administered by that government or its agent, any records of diagnostic and treatment services provided in respect of a patient in an approved hospital;

(b) the board of an approved hospital may disclose any records of diagnostic and treatment services provided in respect of a patient in its hospital to any person without the consent of the patient, for the purpose of being used

(i) in bona fide research or in medical review, if the disclosure is made in such a manner as to ensure confidentiality of those records, or

(ii) for training purposes in a medical records school, if it does so in a manner that the individual names of the patients in those records are not revealed or made identifiable;

(c) the board of an approved hospital shall, after the discharge of a patient from the hospital for the purpose of transferring him to another hospital or nursing home inside or outside Alberta, forward to that other hospital or nursing home copies of the appropriate records of diagnostic and treatment services provided in respect of that patient for the use of the staff of that other hospital or nursing home;

(c.01) repealed 1995 c18 s2;

(c.1) the board of an approved hospital may divulge any records of diagnostic and treatment services provided in respect of a patient to a local board under the *Public Health Act* or a regional health authority or provincial health board under the *Regional Health Authorities Act* if the local board or the regional health authority or provincial health board has assumed the responsibility for any care or treatment of the patient;

(d) repealed 1995 c18 s2;

(d.1) the board of an approved hospital may disclose any records of diagnostic and treatment services provided in respect of a patient to a radiation medical officer or a person authorized in writing by a radiation medical officer under the *Radiation Protection Act* if the disclosure is in accordance with section 15 of that Act and does not interfere with the care of the patient;

(e), (f) repealed 1995 c18 s2;

(g) the board of an approved hospital may divulge any records of diagnostic and treatment services provided in respect of a patient

(i) to the Public Guardian, if the diagnosis, record or information is, in the opinion of the person making the disclosure, relevant to the making of a guardianship order, or

(ii) to the Public Trustee, if the diagnosis, record or information is, in the opinion of the person making the disclosure, relevant to the making of a trusteeship order under the *Dependent Adults Act* in respect of the person to whom the diagnosis, record or information relates;

(h) the board of an approved hospital may divulge any records of diagnostic and treatment services provided in respect of a patient to aboard of review appointed pursuant to the *Criminal Code (Canada)* that is to review the case of the person to whom the records relate; (i) repealed 1995 c18 s2;

(6.1) Notwithstanding subsection (3) or any other law, the board of an approved hospital may, in accordance with subsections (6.2) and (6.3), disclose to an authorized person information respecting diagnostic and treatment services provided to or in respect of a patient.

(6.2) Information may be disclosed under subsection (6.1) only if it is needed for a preliminary investigation, a discipline proceeding or a practice review conducted pursuant to a professional Act.

(6.3) Information may be disclosed under subsection (6.1) only if (a) an officer of an association regulated by a professional Act makes a written request for it and the patient or the patient's legal representative consents to the disclosure, or (b) the disclosure is made by a member of the board of the approved hospital in compliance with a notice, issued pursuant to a professional Act, to attend as a witness or produce documents.

(6.4) For the purposes of subsections (6.1), (6.2), (6.3) and this subsection,

(a) "authorized person" means a person or body that is authorized by a professional Act to conduct a preliminary investigation, a discipline proceeding or a practice review;

(b) "professional Act" means an Act that regulates a profession.

(7) Notwithstanding subsection (3) or any other law, a medical examiner appointed under the *Fatality Inquiries Act* is entitled to inspect and make copies of any diagnosis, record or information relating to a patient.

(8) Repealed 1985 c26 s7.

(9) Notwithstanding subsection (3) or any other law, an Appeal Board is entitled, for the purposes of an appeal under section 36, to inspect and make copies of any diagnosis, record or information relating to a patient and may admit a copy of the diagnosis, record or information in evidence at the appeal, but all proceedings related to the diagnosis, record or information shall be held in private.

(10) Notwithstanding subsection (3) or any other law, if a board, an employee of the board, the Minister or a person authorized by the Minister, a physician or a member of a professional staff

(a) is unable to divulge any diagnosis, record or information relating to a patient by reason of subsection (3), or
(b) refuses to divulge any diagnosis, record or information relating to a patient pursuant to subsection (5), the patient or his legal representative may apply to the court for an order directing the person having the diagnoses, records or information to release them or a copy of them to the patient or his legal representative or to some other person named in the order.

(11) An application under subsection (10) shall be made (a) on motion in the course of any action or proceedings to which the patient or his legal representative is a party, to a judge of the court in which the action or proceeding is taken, or (b) by way of originating notice to the Court of Queen's Bench in any other case.

(12) An application under subsection (10) shall be heard in private and on the hearing of the motion the onus of showing why the order

should not be made for the release of the diagnoses, records or information, or a copy of them, is on the respondent to the motion.

(13) In this section,

(a) "legal representative" means an executor or administrator of the estate of a deceased person, the guardian or trustee of a dependent adult under the *Dependent Adults Act*, the agent designated in a personal directive made by a person in accordance with the *Personal Directives Act* or the guardian of a minor;

(b) "mentally competent" means able to understand the subject matter in respect of which consent is requested and able to appreciate the consequences of giving or refusing consent.

9. Human Tissue Gift Act – Amends R.S.A. 1980 c. H-12

A. Health Information Act Provision

118(1) The *Human Tissue Gift Act* is amended by this section.

(2) Section 11 is amended by adding the following after subsection (2):

> (3) If there is an inconsistency or conflict between subsection (1) and the *Health Information Act*, subsection (1) prevails.

B. Human Tissue Gift Act Provision

11(1) Except when legally required, no person shall disclose or give to any other person any information or document whereby the identity of a person

> (a) who has given or refused to give a consent,
>
> (b) with respect to whom a consent has been given, or
>
> (c) into whose body tissue has been, is being or may be transplanted, may become known publicly.

(2) When the information or document disclosed or given pertains only to the person who disclosed or gave the information or document, subsection (1) does not apply.

10. Mental Health Act – Amends S.A. 1988 c. M-13.1

A. Health Information Act Provision

119(1) The *Mental Health Act* is amended by this section.

(2) Section 17 is amended

> (a) in subsection (1) by adding the following after clause (b):
>
> > (b.1) "health information" means health information as defined in the *Health Information Act*;
>
> (b) by adding the following after subsection (1):
>
> > (1.1) Except as permitted or required under this Act, the Minister, a person authorized by the Minister, a board, an employee of a board or a physician may disclose health information obtained from records maintained in a diagnostic and treatment centre or from persons having access to them only in accordance with the *Health Information Act*.
>
> (c) in subsection (3)
>
> > (i) in clause (a) by striking out "medical" and substituting "health information";

(ii) by repealing clause (c);

(d) by repealing subsections (4) and (5);

(e) in subsection (5.1) by striking out "Notwithstanding subsection(4) or any other law, the Minister" and substituting "The Minister";

(f) in subsection (6)

(i) by striking out "Notwithstanding subsection (4) or any other law, the Minister" and substituting "The Minister";

(ii) by striking out "diagnosis, record or" wherever it occurs and substituting "health";

(iii) by repealing clauses (a), (b), (c), (g), (k) and(o);

(g) by repealing subsections (7), (9), (10), (11) and (12).

B. Mental Health Act Provision

17(1) In this section,

(a) "board" means the board or person in charge of a diagnostic and treatment centre;

(b) "diagnostic and treatment centre" or "centre" means a place established by the Minister pursuant to section 49(a) or (b) and includes a facility that is not an approved hospital under the Hospitals Act, a hospital under the jurisdiction of a provincial health board under the *Regional Health Authorities Act*;

(c) "legal representative" means an executor or administrator of the estate of a deceased person, the guardian or trustee of a dependent adult under the *Dependent Adults Act*, the agent designated in a personal directive made by a person in accordance with the Personal Directives Actor the guardian of a minor;

(d) "mentally competent" means able to understand the subject matter in respect of which consent is requested and able to appreciate the consequences of giving or refusing consent.

(2) The board of a diagnostic and treatment centre shall cause a record to be kept of the diagnostic and treatment services provided to every person in the diagnostic and treatment centre.

(3) For the purpose of assessing the standards of care furnished to persons in a diagnostic and treatment centre or improving mental healthcare facilities or procedures or enforcing the Crown's right of recovery under Part 5 of the Hospitals Act or for any other purpose considered by the Minister to be in the public interest, the Minister or any person authorized in writing by the Minister may require that all or any of the following be sent to the Minister or any person designated by the Minister:

(a) medical and other records in a centre;

(b) extracts from and copies of those records;

(c) diagnoses, charts or information available in respect of any person receiving diagnostic and treatment services in a centre.

(4) Information obtained from records maintained in a diagnostic and treatment centre or from persons having access to them shall be treated as private and confidential information in respect of the person receiving diagnostic and treatment services in the centre and shall be used solely for the purposes described in subsection (3), and the information shall not be published, released or disclosed in any manner that would be detrimental to the personal interest, reputation or privacy of that person or that person's attending physician or any other person providing diagnostic or treatment services to that person.

(5) Any person who knowingly and willfully releases or discloses information described in subsection (4) to a person not authorized to receive it is guilty of an offence and is liable to a fine of not more than $2000.

(5.1) Notwithstanding subsection (4) or any other law, the Minister or any person authorized by the Minister may, for the purpose of enforcing the Crown's right of recovery under Part 5 of the *Hospitals Act*, disclose information obtained under subsection (3).

(6) Notwithstanding subsection (4) or any other law, the Minister, a person authorized by the Minister, a board, an employee of a board or a physician may disclose any diagnosis, record or information relating to a person receiving diagnostic and treatment services in a centre

(a) to the person to whom the diagnosis, record or information relates or his legal representative,

(b) with the written consent of the person to whom the diagnosis, record or information relates or his legal representative, or without that consent if the person is not mentally competent and does not have a legal representative, to any person, if in the opinion of the person making the disclosure it is in the best interests of the person to whom the diagnosis, record or information relates to disclose that information,

(c) to a department or agency of the Government or to a physician if that department, agency or physician is responsible for providing continued treatment to the person to whom the diagnosis, record or information relates,

(d) to the Public Guardian if the diagnosis, record or information is, in the opinion of the person making the disclosure, relevant to the making of a guardianship order under the *Dependent Adults Act* in respect of the person to whom the diagnosis, record or information relates,

(e) to the Public Trustee if the diagnosis, record or information is, in the opinion of the person making the disclosure, relevant to the making of a trusteeship order under the Dependent Adults Act in respect of the person to whom the diagnosis, record or information relates,

(f) to a review panel that is to hear or is hearing an application from the person to whom the diagnosis, record or information relates, or to the Court of Queen's Bench for the purposes of an appeal under section 43,

(g) to a person conducting bona fide research or a medical review if the disclosure is made in a manner that ensures confidentiality of the diagnosis, record or information,

(h) to a Director of Medical Services under the *Occupational Health and Safety Act* when the diagnosis, record or information relates to an accident that occurred in respect of the person's occupation or one or more of his former occupations, or to a disease that is related to the person's occupation or one or more of his former occupations,

(i) to The Workers' Compensation Board, the Provincial Health Authorities of Alberta or a provincial hospital insurance authority if the information is required in order to establish responsibility for payment,

(j) to the Department of National Health and Welfare (Canada) for purposes in connection with the *Canada Health Act (Canada)*,

(k) to a medical records school for training purposes if the disclosure is made in such a manner that names and identities of the persons to whom the records relate are not revealed or made identifiable,

(l) to a board of review appointed pursuant to the *Criminal Code(Canada)* that is to review the case of the person to whom the diagnosis, record or information relates,

(m) to the council of the College of Physicians and Surgeons or an investigating committee under the *Medical Profession Act* or the Professional Conduct Committee or the Appeals Committee under the Nursing Profession Act, if

  (i) an officer of the College or the Alberta Association of Registered Nurses, as the case may be, makes a written request for the diagnosis, record or information and the disclosure is consented to by the person to whom the diagnosis, record or information relates or his legal representative, or

(ii) the disclosure is made in compliance with a notice under section 49 of the *Medical Profession Act* or section 72 of the *Nursing Profession Act* to attend as a witness or to produce documents,

(n) to a person conducting a preliminary investigation, the Discipline Committee or the Board under the *Dental Profession Act* if

(i) an officer of The Alberta Dental Association makes a written request for it and the disclosure is consented to by the patient or his legal representative, or

(ii) the disclosure is made in compliance with a notice under section 56 of the *Dental Profession Act* to attend as a witness or to produce documents,

(o) to a local board under the *Public Health Act* or a regional health authority or provincial health board under the *Regional Health Authorities Act* if the local board or regional health authority or provincial health board has assumed responsibility for any care or treatment of the patient,

(p) to the Health Disciplines Board or

(i) to the Committee of a designated health discipline governed by a Committee, or

(ii) in the case of a designated health discipline governed by a health discipline association, to the conduct and competency committee established by the health discipline association, if the disclosure is made in compliance with a notice under section 18(1) of the Health Disciplines Act, and

(q) to a person conducting a preliminary investigation or the Discipline Committee under the *Psychology Profession Act* if

(i) an officer of the College of Alberta Psychologists makes a written request for it and the disclosure is consented to by the patient or his legal representative, or

(ii) the disclosure is made in compliance with a notice under section 41 of the *Psychology Profession Act* to attend as a witness or to produce documents.

(7) Notwithstanding subsection (4) or any other law, if the Provincial Court issues a subpoena pursuant to the *Child Welfare Act*, a physician, aboard, an employee of a board, the Minister or a person authorized by the Minister shall release, in accordance with that Act, any diagnosis, record or information in respect of the child to whom the proceedings before the Provincial Court relate or with respect to a guardian of that child.

(8) The person in charge of a diagnostic and treatment centre shall, after the discharge of a patient from the centre for the purpose of transferring him to another centre, hospital or nursing

home inside or outside Alberta, forward to that other centre, hospital or nursing home copies of the appropriate records of diagnostic and treatment services provided in respect of that patient for the use of that other centre, hospital or nursing home.

(9) Notwithstanding subsection (4) or any other law, a medical examiner appointed under the *Fatality Inquiries Act* is entitled to inspect and make copies of any diagnosis, record or information relating to a person receiving diagnostic and treatment services in a centre.

(10) Notwithstanding subsection (4) or any other law, when the Minister, a person authorized by the Minister, a board, an employee of a board, or a physician

- (a) is unable to disclose any diagnosis, record or information relating to a person by reason of subsection (4), or
- (b) refuses to disclose any diagnosis, record or information relating to a person pursuant to subsection (6), the person or his legal representative may apply to a court for an order directing the person having the diagnosis, record or information to release it or a copy of it to the person to whom the information relates or his legal representative or to some other person named in the order.

(11) An application under subsection (10) shall be made (a) on motion in the course of any action or proceedings to which the person to whom the diagnosis, record or information relates or his legal representative is a party, to a judge of the court in which the action or proceedings are taken, or (b) by way of originating notice to the Court of Queen's Bench, in any other case.

(12) An application under subsection (10) shall be heard in private and on the hearing of the motion the onus of showing why the order should not be made for the release of the diagnosis, record or information, or a copy of it, is on the respondent to the motion.

11. Nursing Homes Act - Amends S.A. 1985 c. N-14.1

A. Health Information Act Provision

120(1) The *Nursing Homes Act* is amended by this section.

(2) Section 27 is amended by adding the following after subsection (3):

> (4) Subsection (2) does not apply to health information as defined in the *Health Information Act*.

B. Nursing Homes Act Provision

27(1) An operator shall cause to be kept a record in respect of each resident and his property as prescribed by the regulations.

(2) Information in a resident's record shall be treated as private and confidential information and, except as prescribed by the regulations, shall not be published, released or disclosed in any manner that would be detrimental to the personal interest, reputation or privacy of a resident or person caring for a resident.

(3) A person who knowingly and willfully releases or discloses information obtained from a resident's record to a person not authorized to receive the information is guilty of an offence and liable to a fine of not more than $500.

12. Pharmacy and Drug Act – Amends S.A. 1999 c. P-7.3

A. Health Information Act Provision

121 The *Pharmacy and Drug Act* is amended by adding the following after section 47:

> 47.1 The *Health Information Act* is amended in the following provisions by striking out "*Pharmaceutical Profession Act*" and substituting "*Pharmacy and Drug Act*":
>
> section 1(1)(f)(x);
> section 1(1)(f)(xi);
> section 1(1)(h)(iv);
> section 1(1)(l)(ii).

13. Protection for Persons in Care Act - Amends S.A. 1995 c. P-19.5

A. Health Information Act Provision

122(1) The *Protection for Persons in Care Act* is amended by this section.

(2) Section 7(5)(b) is amended by striking out "the medical or clinical records of a person" and substituting "a person's health information records within the meaning of the *Health Information Act*".

B. Protection for Persons in Care Act Provision

7(1) For the purposes of conducting an investigation, an investigator may enter an agency at any reasonable hour.

(2) An investigator, in conducting an investigation, is entitled to access to the records of the agency for the purpose of inspecting them, making copies of them or taking extracts from them.

(3) If the investigator is refused entry to an agency for the purposes of conducting an investigation, the appropriate Minister or a person designated by the Minister may apply to the Court of Queen's Bench by originating notice for an order permitting the investigator to

> (a) enter the agency at any reasonable hour and conduct the investigation, and
>
> (b) require the production of any records of the agency.

(4) An application under subsection (3) may be made ex parte if the Court considers it proper to do so in the circumstances.

(5) Subsections (2) and (3) do not apply to

(a) the financial records of the agency that relate to the operation of the agency, or

> (b) the medical or clinical records of a person unless that person or that person's guardian consents to those records being inspected.

14. Public Health Act - Amends S.A. 1984 c. P-27.1

A. Health Information Act Provision

123(1) The *Public Health Act* is amended by this section.

(2) Section 63(4)(d) is repealed.

(3) Section 83 is repealed and the following is substituted:

> 83 Except for the *Alberta Bill of Rights*, this Act prevails over any enactment that it conflicts or is inconsistent with, including the *Health Information Act*, and a regulation under this Act prevails over any other by-law, rule, order or regulation with which it conflicts.

B. Public Health Act Provision

63(4) Information obtained by the Chief Medical Officer or by a regional health authority or an employee or agent on its behalf may be disclosed by the Chief Medical Officer or the regional health authority, employee or agent

> (d) to a person conducting bona fide research or medical review if the disclosure is made so as to ensure confidentiality of the information;

83 This Act prevails over any enactment with which it conflicts, other than the Alberta Bill of Rights, and a regulation under this Act prevails over any other by-law, rule, order or regulation with which it conflicts.

15. Regional Health Authorities Act - Amends S.A. 1994 c. R-9.07

A. Health Information Act Provision

124(1) The *Regional Health Authorities Act* is amended by this section.

(2) Section 21(1)(o) is repealed.

B. Regional Health Authorities Act Provision

21(1) The Lieutenant Governor in Council may make regulations

(o) respecting the confidentiality requirements to be observed by a person with respect to information obtained in the administration of this Act or in providing health services or health related services under this Act;

APPENDIX 1

Health Information Act Forms

1. Request to Access Health Information
2. Authorization of Representative and Affidavit for Witness
3. Access Request Review Form
4. Access Request Recommendation Form
5. Request to Correct or Amend Health Information
6. Sample Collection Notice
7. Consent to Disclosure (Section 34)
8. Consent to Disclosure (Section 59)
9. Notice to Recipient (Disclosure with Consent)
10. Notice to Recipient (Disclosure without Consent)
11. Notice to Recipient (Non-Custodian)
12. Components for an Affiliates Oath of Confidentiality
13. Request for Review (Office of the Information and Privacy Commissioner)

Alberta's Health INFORMATION Act

Request to Access Health Information

The information on this form is collected under Alberta's *Health Information Act* and will be used to respond to your request for your own health information. Instructions for completing this form are on the back.

About you

☐ Mr. ☐ Ms ☐ Dr. ☐ Mrs. ☐ Miss	Last name		First name
Mailing address			
City or town		Province	Postal code
Telephone (business) ( )	Telephone (home) ( )	Fax number ( )	E-mail address
Date of Birth (day) (month) (year)	Other		

About your request

1. Please attach the initial fee of $25.00.
2. To which custodian are you making your request? *(Please fill in the name of the individual or organization.)*

3. Do you want to: (a) receive a copy of the record? ☐ **OR** (b) examine the record? ☐

About the information you want to access

1. What records do you want to access? Please give as much detail as possible. Indicate if you also want access to records about the disclosure of your information. *(Be sure to give all your previous names. If you are requesting access to another individual's information, you must include information to identify the individual (in the box below) and attach proof that you can legally act for that individual (under section 104 of the Act). If you need more space, please attach a separate sheet of paper.)*

2. What is the time period of the records? Please give specific dates. *(See reverse for details.)*

Your signature

Signature	Date

For authorized office use only:

Date received	Request number

How to complete the form

You may be able to access your own health information without making a request under the *Health Information Act*. To determine whether you need to make a request under the *Act* or if you need help completing the form, contact the HIA Coordinator or the person responsible for processing requests in the organization to whom you are making the request.

About you

Check the title by which you prefer to be addressed and enter your last name and first name. Enter your complete mailing address and your daytime and evening telephone numbers. The custodian may need to contact you if they have any questions about your request. If you have a fax number or E-mail address where correspondence can be sent, enter them in the spaces provided.

About your request

If you need help to find out what records a custodian has, please consult their HIA Coordinator or the person responsible for processing requests.

1. If you are making a request for your own health information you will have to provide proof of your identity before the records are released to you. If you are requesting records for another person, you will have to provide proof that you have the authority to act for that person. For example, you might provide proof that you are the person's guardian or trustee or that you have power of attorney for the person. There will be an initial fee of $25. If additional fees are charged, you will be provided with an estimate of how much your request will cost before processing begins. Processing starts once you have paid at least 50% of any estimated fee. The records are provided when the fee is paid in full.

2. Enter the name of the custodian that you believe has the records that you want to access.

3. Do you want to receive a copy of the record or examine the record? Check the appropriate box.

About the information you want to access

1. What health information are you requesting? Please be as specific as possible in describing the records. The more specific your request, the quicker and more accurately it can be answered. If you need more space, please continue your description on a separate sheet of paper and attach it to this request form.

   Please be sure that you give:
   - your full name;
   - any other names that you have previously used; and
   - any identifying number that relates to the records, such as your personal health number, case number or other identification number.

   If you are requesting records for another person, you will have to provide proof that you have the authority to act for that person.

2. Enter the time period of the requested records. For example, if you are requesting records for the period January 1, 1998 to August 31, 1999, enter those dates in the space provided. If you want records from August, 1996 to the present, enter "August, 1996 to the present."

Your signature

Sign and date the form and send it to the HIA Coordinator or person responsible for processing requests. If you are not sure of where to send the form, please consult the HIA Coordinator or other responsible person of the organization that has the records you wish to access.

Authorization of Representative
(Under Section 104(1)(i))

I, ______________________________, living at ______________________________,

______________(name of municipality), in the province of ______________________________,

designate ____

living at ______________________________(name of municipality) in the province of

______________________________as my authorized representative to act on my behalf,

and to exercise (check one of the following):

☐ all my rights under the *Health Information Act;* OR

☐ my right to access all records containing my health information; OR

☐ other – define:

____

____

☐ the rights that are conferred on me under the *Health Information Act* in regard to the following questions:

____

____

I confirm that my representative has the authority to carry out the above rights and responsibilities on my behalf.

The present authorization will be in effect until ______________________, 20_____.

SIGNED BY ______________________________ in the presence of:

____
Witness

Affidavit for Witness (Optional)

Canada
in the Province of Alberta

I ____________________, __________________ of ____________________________
(name of the witness in full) (occupation of witness) (complete home address of witness)

in the province of ____________________________________, make oath and say that:

1. I was personally present and I saw ______________________________ sign the
(name of person)
Authorization of Representative to which this is attached.

2. The Authorization of Representative was signed by ________________________
(name of the person)
at _________________________________ in the province of
________________________ and that I am the one who witnessed the document.

3. I know __________________ and I believe that he/she is 18 years of age or older.
(name of person)

____
Signature of Witness

Sworn before me at _________________________

in the province of __________________________

on ____

____
Commissioner for Oaths

____
(print name here)

My Commission expires ________________, 20___

Alberta's Health INFORMATION Act

HEALTH INFORMATION ACT

ACCESS REQUEST REVIEW

NAME OF CUSTODIAN

Where are the Records Held?	**Request No.:**

PART 1 - GENERAL

METHOD OF ACCESS REQUESTED

☐ Examine Originals ☐ Copies (selected documents) ☐ Copies (all) ☐ Other (specify): ____________________

TRACKING DATES

Date Received	Request Due Date	Revised Due Date	Request Closed Date

AREA(S) ASSIGNED TO PROCESS REQUEST

SUMMARY OF STAFF TIME SPENT ON REQUEST

Locate Records	Review Records	Sever Records	Prepare Response Pkg.	Name(s)	Total Hours Spent (min. ¼ hour)
☐	☐	☐	☐	____________________	________
☐	☐	☐	☐	____________________	________
☐	☐	☐	☐	____________________	________
☐	☐	☐	☐	____________________	________

SUMMARY OF RECOMMENDATIONS FROM HIA COORDINATOR

(Attach a separate sheet if the space below is not sufficient.)

Prepared by: (type name and sign)	**Approved by:** (type name and sign) **HIA Coordinator or Responsible Affiliate**
Title:	**Date:**

ACCESS REQUEST REVIEW - PAGE 2

NAME OF CUSTODIAN:

Request No.:

PART 2: RETRIEVAL AND REVIEW OF RECORDS

Area Where Records Located:	**Contact Person:**	**Telephone No.:**

LOCATION AND RETRIEVAL OF RECORDS

Search Done By: **(name in print)**	**Start Date:**	**Target Completion Date:**	**Actual Completion Date:**

Areas Searched (attach file lists, indices or other aids used in search):

Records Retrieved (by title - use attachment if necessary):

REVIEW OF RECORDS BY AREA HOLDING RECORDS

Records Reviewed By: **(name in print)**	**Start Date:**	**Target Completion Date:**	**Actual Completion Date:**

SUMMARY OF RECOMMENDATIONS FROM AREA HOLDING RECORDS

Approved By:
(type name and sign)

Date:

Alberta's Health
INFORMATION
Act

ACCESS REQUEST RECOMMENDATION

NAME OF CUSTODIAN

Where are the Records Held?	**Request No.:**
To:	**Date:**
From:	**Name of Applicant:**
Records / Information Requested:	**Number of Files / Pages Reviewed:**

Types of Health Information Contained in the Records:

Exceptions Recommended:

Application of Discretionary Exceptions (summarize reasons):

Application of Mandatory Exceptions (summarize reasons):

Severing Required (summarize reasons):

Prepared by: (signature)		**Approved by:** (signature)	
Title:	**Date:**	**Title:**	**Date:**

NAME OF CUSTODIAN
ACCESS REQUEST RECOMMENDATION: DETAILED REVIEW OF RECORDS

(use multiple sheets if necessary)

Request No.:	**Name of Custodian:**	**Area Holding Records:**	**Contact Person:**	**Telephone No.:**

Document No.	**No. of Pages**	**Document Date**	**Document Description**	**Exceptions Applied (Section #'s)**	**Comments / Explanations**	**Consultation (Yes or No)**

Alberta's Health INFORMATION Act

Request to Correct or Amend Health Information

The information on this form is collected under Alberta's *Health Information Act* and will be used to respond to your request for correction or amendment. Instructions for completing this form are on the back.

About you

☐ Mr. ☐ Ms ☐ Dr. ☐ Mrs. ☐ Miss	Last name		First name
Mailing address			
City or town		Province	Postal code
Telephone (business) ( )	Telephone (home) ( )	Fax number ( )	E-mail address
Date of Birth (day) (month) (year)			

About your request

1. Whose information do you want to correct?

☐ Your own health information

☐ Another person's health information *(Please include information to identify the other individual and attach proof that you can legally act for the individual (section 104 of the Act)*

2. To which custodian are you making your request? *(Please fill in the name of the individual or organization.)*

About the information you want to correct

1. What health information needs to be corrected or amended? Please give as much detail as possible. *(Be sure to give the complete name that is in the records if it is different from the name given above. If you need more space, please attach a separate sheet of paper.)*

2. What correction or amendment do you want to make and why? *(Please attach any documents that support your request.)*

Your signature

Signature	Date

For authorized office use only:

Date received	Request number

How to complete the form

You can correct or amend information in many custodian records without making a request under the *Health Information Act*. To determine whether you need to make a request under the *Act* or if you need help completing the form, contact the HIA Coordinator or the person responsible for processing requests in the organization to whom you are making the request.

About you

Check the title by which you prefer to be addressed and enter your last name and first name. Enter your complete mailing address and your daytime and evening telephone numbers. The custodian may need to contact you if they have any questions about your request. If you have a fax number or E-mail address where correspondence can be sent, enter them in the spaces provided.

About your request

1. Whose information do you want to correct or amend? Indicate whether you want your health information or another person's health information to be corrected.

   Your health information: If you want your records to be corrected or amended, you will have to provide proof of your identity.

   Another person's health information: If you want the records of another person to be corrected or amended, you will have to provide proof that you have the authority to act for that person. For example, you might provide proof that you are the person's guardian or trustee or that you have power of attorney for the person.

2. Enter the name of the custodian that you believe has the records that you want to correct or amend.

About the information you want to correct

1. What records contain the information that you want corrected or amended? Please be as specific as possible in describing the records. The more specific your request, the quicker and more accurately it can be answered. If you need more space, please continue your description on a separate sheet of paper and attach it to this request form.

   If you want a correction or amendment made to your own health information, please be sure that you give:
   - your full name;
   - any other names that you have used on the records; and
   - any identifying number that relates to the records, such as your personal health number, case number or other identification number.

   If you want a correction made to another person's information, please give:
   - the person's full name;
   - any other name that person may have used on the records; and
   - any identifying numbers (such as a personal health number, case number, etc.) for the person if you know them.

2. What corrections or amendments do you want made? What is incorrect about the information that is currently on the record? Please be specific.

Your signature

Sign and date the application and send it to the HIA Coordinator or personal responsible for processing requests in the appropriate organization. If you are not sure of where to send the form, please consult the HIA Coordinator or responsible person in the organization that has the records you wish to correct or amend.

SAMPLE COLLECTION NOTICE (SECTION 22(3))

For the purposes of section 22(3), a collection notice may be:

- explained orally to individuals;
- added to the top of a questionnaire or application form;
- put in a publication (e.g. brochure) or other information about a program or service and provided to individuals;
- put in a poster on a physician's office or pharmacy wall; or
- put in a pop-up screen as part of a computer program

An example of a collection notice is as follows:

"The health information that we are collecting is needed to determine your eligibility for the ______________ program, service or benefit (or to provide you with diagnostic, treatment and care services) (or for the training of students) (or for research or statistical purposes) (or for other authorized purpose(s) under section 27 of the *Health Information Act*). It is collected under the authority of the (Mental Health Act) (or Cancer Programs Act) (or Hospitals Act) (or Nursing Homes Act) (or Alberta Health Care Insurance Act) (and/or section 20(b) of the *Health Information Act* – directly related to and necessary to carry out an authorized purpose under section 27) (or other legal authority). The confidentiality of this health information and your privacy are protected by the provisions of the *Health Information Act* (and any other act that is appropriate to add).

If you have any questions about this collection and use of your health information, please talk to one of the staff (or contact) ____________ (position) at ___________ (business address) or phone ____________ (business phone)."

CONSENT TO THE DISCLOSURE OF INDIVIDUALLY IDENTIFYING HEALTH INFORMATION

(AUTHORIZED BY SECTION 34 OF *HIA*)

I, ____, authorize (the attached) individually identifying

- ☐ diagnostic, treatment and care information
- ☐ registration information
- ☐ health services provider information

of myself to be disclosed by ____(name of custodian), in accordance with section 34 the *Health Information Act* to, ________________ _______________________________ (name of recipient), for the following purpose (s):

____

____

____

____

____

____

I understand why I have been asked to disclose my individually identifying information, and am aware of the risks or benefits of consenting, or refusing to consent, to the disclosure of my individually identifying information. I understand that I may revoke this consent at any time.

Dated this ____________________ of __________________ , __________________.
(day) (month) (year)

Expiry date (if any) ____________________ of __________________, __________________.
(day) (month) (year)

____
Client or Authorized Representative's Signature

____
Source of Representative's Authority
(refer to section 104(1) of the *Act*)

____
Client or Authorized Representative's Name

____
Witness Signature

____
Witness Name

CONSENT TO THE DISCLOSURE OF INDIVIDUALLY IDENTIFYING DIAGNOSTIC, TREATMENT AND CARE INFORMATION BY ELECTRONIC MEANS (AUTHORIZED BY SECTION 59 OF *HIA*)

I, ______________________________ (Personal Health Number ______________________) authorize my individually identifying diagnostic, treatment and care information to be disclosed by custodians in accordance with the *Health Information Act (HIA)* by computer systems that facilitate access by authorized persons to electronic or digital information that is stored in a computer database by a custodian. I understand that my consent is not required for disclosure of my information in other electronic ways including fax, e-mail, Intranet or Internet communications. By authorizing my information to be disclosed by electronic means (as defined above), my information may be used by:

(1) all custodians for:

- providing a health service to me
- determining or verifying my eligibility to receive a health service
- conducting investigations, discipline proceedings, practice reviews or inspections relating to the members of a health profession or health discipline that have provided a health service to me
- conducting research, subject to any requirements placed upon them by an ethics committee designated by the Minister of Alberta Health and Wellness
- providing education programs for health services providers
- carrying out any purpose authorized by an enactment of Alberta or Canada
- carrying out internal management purposes, including planning, resource allocation, policy development, quality improvement, monitoring, audit, evaluation, reporting, obtaining or processing payment for health services and human resource management

(2) the Minister of Alberta Health and Wellness, the Department of Alberta Health and Wellness, regional health authorities, the Alberta Mental Health Board and the Alberta Cancer Board for planning and resource allocation, health system management, public health surveillance and health policy development in the geographic area, and for the health programs, for which they are responsible.

I understand the custodians that access my individually identifying diagnostic, treatment and care information by these computer systems will do so according to their obligations in the *Health Information Act* and that my information will be stored securely, subject to the requirements of the *Health Information Act*.

I understand why I have been asked to disclose my individually identifying diagnostic, treatment and care information in this way, and am aware of the risks or benefits of consenting, or refusing to consent, to the disclosure of my individually identifying diagnostic, treatment and care information in this way. I understand that I may revoke this consent at any time.

I authorize my consent information (i.e. the fact that I have consented under section 59 of *HIA*) to be disclosed to custodians under the *Health Information Act.*

Dated this ______________________ of __________________ , __________________.
(day) (month) (year)

____
Client or Authorized Representative Signature

____
Source of Representative's Authority
(Refer to s. 104(1)(c) to (i) of *HIA*)

____
Client or Authorized Representative's Name

____
Witness Signature

____
Witness Name

SECTION 42 NOTICE TO RECIPIENT TO ACCOMPANY THE DISCLOSURE OF INDIVIDUALLY IDENTIFYING DIAGNOSTIC, TREATMENT AND CARE INFORMATION BY A CUSTODIAN

Disclosure with the Subject's Consent

The attached individually identifying diagnostic, treatment and care information of
______________________________ (subject of information) is being disclosed to
______________________________ (name of recipient) by
______________________________ (name of custodian) on
______________________ (date), with the consent of
______________________(name of the subject) under section 34 of the *Health Information Act,* only for the following purpose (s):

____

____

____

____

____

____

____

____

______________________________ ______________________

Name and Signature of Custodian (or affiliate) Date

SECTION 42 NOTICE TO RECIPIENT TO ACCOMPANY THE DISCLOSURE OF INDIVIDUALLY IDENTIFYING DIAGNOSTIC, TREATMENT AND CARE INFORMATION BY A CUSTODIAN

Disclosure Without the Subject's Consent:

The attached individually identifying diagnostic, treatment and care information of ______________ ________________ (named individual subject) has been disclosed to ________________________ __________________ (name of recipient) by _________________________________ (name of custodian) on __________________________________ (date), without the consent of the subject, but authorized under the following provision of the *Health Information Act* (mark the appropriate box)

- ☐ To provide continuing treatment and care to the above individual (s.35(1)(b))
- ☐ To provide information concerning the presence, location, condition, diagnosis, progress and prognosis of the above individual on the above date and the above individual has not requested otherwise (s.35(1)(c)) (Note – recipient must be a family member or another person with whom the individual is believed to have a close personal relationship)
- ☐ To advise family members of the above individual, or a person with whom the above individual is believed to have a close personal relationship, that the individual has been injured, is ill or has died and the individual has not requested otherwise (s.35(1)d))
- ☐ To provide health services to the above individual who is being detained in a penal or other custodial facility (s.35(1)(e))
- ☐ To conduct an audit of the information (s.35(1)(f)) (Note – recipient must enter into an agreement with the custodian about non-disclosure and destruction of the information)
- ☐ To carry out quality assurance activities within the meaning of section 9 of the Alberta Evidence Act (s.35(1)(g))
- ☐ To provide information for a court proceeding or a proceeding before a quasi-judicial body (s.35(1)(h) (Note – the custodian must be a party to the proceeding)
- ☐ To comply with a subpoena, warrant or court order compelling the production of information or with a rule of court that relates to the production of information (s.35(1)(i)) (Note – the recipient body must have jurisdiction to compel the production of information)
- ☐ To investigate an offence involving a life-threatening personal injury to the above individual and the above individual has not requested otherwise (s.35(1)(j) (Note – the recipient must be a municipal or provincial police service)
- ☐ To detect or prevent fraud, limit abuse in the use of health services or prevent the commission of an offence under an enactment of Alberta or Canada (s.35(1)(k)) (Note the recipient must be another custodian)
- ☐ To enable an officer of the Legislature (e.g. Auditor General, Ombudsman, Chief Electoral Officer, Information and Privacy Commissioner) to carry out his/her duties (s.35(1)(l))
- ☐ To avert or minimize an imminent danger to the health or safety of any person (s.35(1)(m))
- ☐ To act in the best interests of the above individual if the individual lacks the mental capacity to provide consent (s.35(1)(n))
- ☐ To provide necessary health services to a descendant of a deceased individual (s.35(1)(o)) (Note – the recipient must be a descendant or a representative under section 104(1)(c) to (i) and the privacy of the deceased individual must be protected)
- ☐ To comply with another act or regulation of Alberta or Canada that authorizes or requires the disclosure (s.35(1)(p))
- ☐ To transfer records to a successor custodian because the first custodian is ceasing to be a custodian (s.35(1)(q))
- ☐ To enable a health professional body to conduct an investigation, a discipline proceeding, a practice review or an inspection (s.35(4)) (Note—the custodian must comply with other relevant legislation and the health professional body must enter into an agreement with the custodian about non-disclosure and destruction of the information)
- ☐ To allow for permanent preservation and historical research by the Provincial Archives of Alberta or another archives that is subject to this Act or the Freedom of Information and Protection of Privacy Act (s.38) (Note—the custodian must determine that the information has enduring value)
- ☐ To enable the Minister of Health and Wellness to carry out his duties (s.40) (Note – the custodian must determine if the disclosure is necessary or desirable)

____ ______________________________

Name and Signature of Custodian (or affiliate) Date

SECTIONS 42 AND 32(2) NOTICE TO ACCOMPANY THE DISCLOSURE OF NON-IDENTIFYING HEALTH INFORMATION TO A RECIPIENT THAT IS NOT A CUSTODIAN

TO: ______________________________________ (Name of Recipient)

If you intend to use the attached non-identifying health information for data matching, you must notify the Information and Privacy Commissioner (780)(422-6860). The *Health Information Act* defines data matching to mean the creation of individually identifying health information by combining individually identifying or non-identifying health information or other information from two or more electronic databases, without the consent of the individuals who are the subjects of the information. Failure to notify the Commissioner of the intention to data match is an offence under the *Act* and may result in a fine of up to $50,000.

____

Name and Signature of Custodian (or affiliate)

____

Date

COMPONENTS FOR AN AFFILIATE'S OATH OF CONFIDENTIALITY

- a statement, sworn (or affirmed) by the affiliate, stating that:
    - he/she will uphold to the best of his/her ability his/her duties under the *Health Information Act* and Regulations and the custodian's policies and procedures; and that
    - he/she will not disclose or make known any recorded or non-recorded health information of an individual except as authorized by the *Act*, the Regulations and the custodian's policies and procedures;
- space for the city, town, village, etc. where the oath is sworn;
- space for the date and signature of a witness;
- place for a Commissioner for Oaths to commission the swearing (or affirming) of the Oath (optional)

HEALTH INFORMATION ACT
REQUEST FOR REVIEW

To: **Information and Privacy Commissioner**
Suite 410, 9925 – 109 Street
Edmonton, Alberta T5K 2J8

My Name Is:

My Mailing Address Is:

A telephone number where I can
be reached during the day is:

On __________ I applied for my own health information from the following source:
Date

OR:

On __________ I asked to have my own health information corrected or amended by the following source:
Date

OR:
I am concerned about the following:

AND:
I am requesting a review by the Commissioner because:

(Please attach a copy of any correspondence you have received from the source you referred to.)

Signature

Date

If you have any questions, please call (422-6860)

This office will forward a copy of your completed form to the head of the custodian concerned and to any other person who in the opinion of the Commissioner is affected by the request. If concerns arise regarding this procedure, please make them known to the Commissioner as soon as possible.

Date Stamp Information and Privacy
Commissioner

APPENDIX 2

Model Letters

Appendix 2
Model Letters

Introduction

The following sample letters are provided to assist custodians in corresponding with applicants, third parties and others in the processing of access and correction or amendment requests. The sample letters are intended to provide general guidance and may be altered to suit the circumstances of each request.

The letters are as follows:

A Acknowledgment of Request
A.1 Notice of Processing an Access Request under the *FOIP Act*
B Notice Regarding Extension of Time Limit
C Fee Estimate
D Abandonment of a Request
E Response to Access Request – Granting Access
F Response to Access Request – Denial of All or Part of Record(s)
G Response to Access Request – Record Does Not Exist
H Acknowledgment of Receipt of Correction or Amendment Request
H.1 Notice of Processing a Request for Correction or Amendment under the *FOIP Act*
I Notification Concerning a Request for Correction or Amendment
J Notice to Persons in Receipt of Health Information
K Notice Agreeing to Make a Correction or Amendment and Dispensing with Notification of Persons About a Correction or Amendment

Model Letter A – Acknowledgment of Request

Purpose: *To acknowledge receipt of the applicant's request for information, to ask for clarification of a request and/or to request that initial fees be paid in order that the request may be considered complete and processing can commence.*

[*Reference number*]

[*Date*]

[*Applicant's name and address*]

Dear [*Applicant's name*]:

Re: Health Information Act
[*Request under Consideration*]

Your request for access to health information [*describe requested health information*] under the *Health Information Act* was received by [*custodian*] on [*date*].

Option A.1: General Acknowledgment

We will provide the information available to you under the *Act* as quickly as possible. Although the *Act* allows us a maximum of 30 days to respond, we will reply sooner than [*date*], if possible.

Option A.2: Need to Supply More Details

Unfortunately, your request for access to information does not provide sufficient specific details to identify the health records you may be requesting. [*Name of custodian*] cannot begin to process your request until we receive additional information to help us [*identify the record or make the request more specific*]. Please help us to clarify your request by supplying any of the following details of which you are aware:

[*list details you are requesting*]

Option A.3: Failure to Include Basic Fee

Unfortunately, you did not include the basic fee of $25.00. The *Act* allows us 30 days to respond to your request, but this time period will not commence until the basic fee has been received. Please forward the fee to [*appropriate address within the custodian*] as quickly as possible.

The processing of the request will commence immediately upon the receipt of your fee.

Option A.4: Clarification of Request

We have now had an opportunity to discuss your request with you [*state method and date*]. We agreed that the request would now focus on [*describe the information agreed upon*]. If this understanding is not correct, please contact me at [*telephone #*] as soon as possible. This letter serves as a notice that it is this request which [*name of custodian*] is proceeding to process. We will provide the information available to you under the *Act* as quickly as possible. Although the *Act* allows us a maximum of 30 days to respond, we will reply sooner than [*date*], if possible.

Section 73 of the *Health Information Act* provides that you may make a written request to the Information and Privacy Commissioner to review this matter. You have 60 days from the date of this notice to request a review by writing to:

Information and Privacy Commissioner
410, 9925 – 109 Street
Edmonton, Alberta, T5K 2J8.

When requesting a review, please provide the Office of the Information and Privacy Commissioner with the following information:

1. The reference number noted at the top of this notice.
2. A copy of this letter.
3. A copy of your original request form that you sent to [*name of custodian*].

If you have any questions, please write to me or call me at [*telephone number*].

Sincerely,

[*Name*]
[*Title*]

Model Letter A.1 – Notice of Processing an Access Request under the *FOIP Act*

Purpose: *To acknowledge receipt of the applicant's request for information, and to give notice that all or part of the request will be processed under the FOIP Act.*

[*Reference number*]

[*Date*]

[*Applicant's name and address*]

Dear [*Applicant's name*]:

Re: Health Information Act
[*Request under Consideration*]

Your request for access to health information [*describe requested health information*] under the *Health Information Act* (the *Act*) was received by [*custodian*] on [*date*].

Some (or all) of the record(s) you requested contain information to which the *Freedom of Information and Protection of Privacy (FOIP) Act* applies. The request for these record(s) is deemed to be a request under section 7(1) of the *FOIP Act* and that *Act* applies to the processing of your (or that part of your) request.

Please see the attached letter related to your (or that part of your) request [*attach a letter acknowledging receipt of the access request under the FOIP Act – use Model Letter A from Appendix 3 – FOIP Guidelines and Practices (2000)*]

If you have any questions, please write to me or call me at [*telephone number*].

Sincerely,

[*Name*]
[*Title*]

Model Letter B – Notice Regarding Extension of Time Limit

Purpose: To advise an applicant of a time extension taken to process a request.

[*Reference number*]

[*Date*]

[*Applicant's name and address*]

Dear [*Applicant's name*]:

Re: Health Information Act
[*Request under Consideration*]

[*Name of custodian*] received your request for access to information on [*date*].

Normally, [*name of custodian*] responds to a request for information within 30 days after receiving the request. However, in limited circumstances, the *Health Information Act* provides that a custodian may extend this time limit.

Option B.1: Time Extension to Clarify Request

In this case, there is a need for us to obtain more information from you before we can identify the records that deal with your request. We will need a time extension of [*number of days – up to 30 days or longer with Commissioner's permission*] to do this and identify the applicable records.

Option B.2: Consultation with Other Custodians

A preliminary review of the records you have requested indicates that consultations with (an) other custodian(s) may be required before we can fully process your request. This consultation is necessary for us to deal completely with the records that you have requested. We will require a time extension of [*number of days – up to 30 days or longer with Commissioner's permission*] to carry out this process.

Option B.3: Large Number of Records

Your request involves a large number of records. The volume of information involved cannot be processed within the usual 30-day limit. An extension of time of [*number of days – up to 30 days or longer with Commissioner's permission*] will allow [*name of custodian*] to provide you with a complete response to your request.

Model Letter B – Notice Regarding Extension of Time Limit (continued)

[*Conclusion for all options*]

A response to your request will be ready no later than [*proposed date*]. We will try to respond sooner, if possible.

If you have any questions regarding this time extension, please contact [*name and job title*] at [*business address*] or telephone [*number*].

If you feel this time extension is unjustified, section 73 of the *Health Information Act* provides that you may ask the Information and Privacy Commissioner to review this decision. You have 60 days from the date of this notice to request a review by writing to:

Information and Privacy Commissioner
410, 9925 – 109 Street
Edmonton, Alberta, T5K 2J8.

When requesting a review, please provide the Office of the Information and Privacy Commissioner with the following information:

1. The reference number quoted at the top of this notice.
2. A copy of this letter.
3. A copy of your original request for information that you sent to [*name of custodian*].

If you have any questions, please write or call me at [*telephone number*].

Sincerely,

[*Name*]
[*Title*]

Model Letter C – Fee Estimate

Purpose: To advise an applicant of the amount of fees that will be involved in processing a request.

[*Reference number*]

[*Date*]
[*Applicant's name and address*]

Dear [*applicant's name*]:

Re: Health Information Act
[*Request under Consideration*]

[*Name of custodian*] received your request for access to health information [*describe requested health information*] on [*date*]. Section 67 of the *Health Information Act Act* provides that fees may be charged for providing you with the information which you requested.

Fees, over and above the basic fee paid at the time you made the request, are assessed because [*provide rationale for fees being assessed*].

The fee for providing the health records you have requested is estimated to be [*$ amount*]. We have calculated this amount as follows:

[*provide calculation*]

Option C.1: Deposit

Please reply to us in writing within 20 days of the date of this notice indicating that you accept this estimate and enclose a deposit of [*$ amount*][*do not send cash*] made payable to [*the appropriate officer of custodian*]. This reply must be sent to [*name of officer, office and address of custodian*] and should quote the reference number provided at the top of this letter. When we have received your response and deposit, processing of your request will continue.

Option C.2: No Deposit

Please reply to us in writing within 20 days of the date of this notice indicating that you accept this estimate and will pay these fees when requested to do so. Please send the reply to [*name of officer, offices and address of custodian*] and quote the reference number provided at the top of this letter. When we have received your response, processing of your request will continue. Please do not send cash.

Model Letter C – Fee Estimate (continued)

Option C.3: Refusal of Request to Excuse Fee

Your request for excusing the payment of the fee cannot be granted [*state reason*]. Please reply to us in writing within 20 days of the date of this notice indicating that you accept this estimate and enclose a deposit of [*specify amount*] [*do not send cash*]. Please send the reply to [*name of officer, offices and address of custodian*] and quote the reference number provided at the top of this letter. When we have received your response, your request will be processed.

If you find the fees a burden to you, we would be pleased to discuss approaches to processing the request which may reduce the fees and still provide the information you require. Please write or call [*name, title, address and telephone number*], who may be able to assist you.

[*For options C.1 and C.2*]

Section 67(4) provides some limited situations where fees can be excused, if you cannot afford to pay the fee or if, in the opinion of the custodian, it is fair to excuse payment. If you believe that one of these circumstances applies to you, you should raise it with the officer mentioned above.

[*Conclusion for all options*]

Section 73 of the legislation allows you to ask the Information and Privacy Commissioner to review this fee estimate and any decision made on a request for excusing of a fee payment. The *Act* allows you 60 days from the date you receive this notice to request a review by writing to

Information and Privacy Commissioner
410, 9925 – 109 Street
Edmonton, Alberta, T5K 2J8.

When requesting a review, please provide the Office of the Information and Privacy Commissioner with the following information:

1. The reference number quoted at the top of this notice.
2. A copy of this letter.
3. A copy of your original request for information that you sent to [*name of custodian*].

If you have any questions, please write or call the officer named above or myself at [*telephone number*].

Sincerely,

[*Name*]
[*Title*]

Model Letter D – Abandonment of Request

Purpose: *To inform the applicant that his or her request is going to be considered abandoned under section 9.*

Note: *The time line to allow the applicant to reactivate the request within 12 months is a suggested guideline, not a requirement of the Act. Custodians may choose to alter this according to the nature of the request or the records involved.*

[*Reference number*]

[*Date*]

[*Applicant's name and address*]

Dear [*Applicant's name*]:

Re: Health Information Act
[*Request under Consideration*]

Option D.1: Abandonment Indicated

You indicated to us on [*date*] that you were abandoning your request [*reference number and subject*]. If you wish to reactivate your request at any time up to [*date 12 months from the date of closure*], you may do so without making another request or submitting an initial fee. After that date, you will have to submit another request and any initial fee that may be required.

Option D.2: Abandonment Not Indicated

We have not received any communication concerning your request since [*date of letter seeking further information or requesting fee*]. For this reason, we are closing the file on your request [*reference number and subject*]. If you wish to reactivate your request at any time up to [*date 12 months from the date of closure*], you may do so without making another request or submitting an initial fee. After that date, you will have to submit another request and any initial fee that may be required.

Model Letter D – Abandonment of Request (continued)

If you disagree with this decision, section 73 of the *Health Information Act* provides that you may ask the Information and Privacy Commissioner to review this decision. You have 60 days from the date of this notice to request a review by writing to:

Information and Privacy Commissioner
410, 9925 – 109 Street
Edmonton, Alberta, T5K 2J8.

When requesting a review, please provide the Office of the Information and Privacy Commissioner with the following information:

1. The reference number quoted at the top of this notice.
2. A copy of this letter.
3. A copy of your original request for information that you sent to [*name of custodian*].

If you have any questions, please write or call me at [*telephone number*].

Sincerely,

[*Name*]
[*Title*]

Model Letter E – Response to Access Request – Granting Access

Purpose: To inform an applicant that access will be granted.

[*Reference number*]

[*Date*]

[*Applicant's name and address*]

Dear [*Applicant's name*]:

Re: Health Information Act
[*Request Under Consideration*]

I am responding to your request of [*date*] for access to health information [*describe requested information*]. We are pleased to provide access to [*specify subject and records generally*].

Option E.1: Copy Enclosed

A copy of the information is enclosed.

Option E.2: Applicant to View Originals

You have requested an opportunity to examine the original records containing your health information rather than receive copies of them. We invite you to examine the record(s) at [*place and address*] on [*date*] at [*time*]. If you are unable to examine the records at that time, please contact [*name and telephone number*] to make alternate arrangements.

Option E.3: Records Cannot be Copied

The record(s) containing the health information you have requested cannot be copied because [*provide reason*]. We invite you to examine the original record(s) at [*place and address*] on [*date*] at [*time*]. If you are unable to examine the record(s) at that time, please contact [*name and telephone number*] to make alternate arrangements.

Option E.4: Fees Required

As we informed you in our fee estimate of [*date*], your request has now been processed and fees totaling [*$ amount and calculation, if previous deposit received*] must be paid before access can be provided.

Model Letter E – Response to Access Request – Granting Access (continued)

Please make your cheque or money order payable to [*name of custodian*] and send it to [*name of officer, office and address of custodian*].

If you feel that your request has not been answered completely or that you require further clarification, please contact [*name and job title*] at [*business address and telephone number*].

Under section 73 of the *Health Information Act*, you may ask the Information and Privacy Commissioner to review the assessment of a fee or any other matter concerning this response to your request. You have 60 days from the date of this notice to request a review by writing to:

Information and Privacy Commissioner
410, 9925 – 109 Street
Edmonton, Alberta, T5K 2J8.

If you wish to request a review, please provide the Office of the Information and Privacy Commissioner with the following information:

1. The reference number quoted at the top of this notice.
2. A copy of this letter.
3. A copy of your original request for information that you sent to [*name of custodian*].

If you have any questions, please write or call me at [*telephone number*].

Sincerely,

[*Name*]
[*Title*]

Model Letter F – Response to Access Request – Denial of All or Part of Record(s)

Purpose: To inform an applicant that access to all or part of the records requested has been denied.

[*Reference number*]

[*Date*]

[*Applicant's name and address*]

Dear [*Applicant's name*]:

Re: Health Information Act
[*Request under Consideration*]

I am replying to your request of [*date*] for access to [*describe requested health information*].

Option F.1: Total Denial

Unfortunately, access to all the health information that you requested is refused under section(s) [*put in an explanation, including the detailed sections on which refusal is based (identify exception(s) used from section 11(a) or (b)*].

Option F.2: Some Records Available

I am pleased to inform you that access is being provided to [*specify particular records*].

- A copy of the record(s) containing your health information is attached; or
- You asked to examine the original records containing your health information rather than receive copies. We invite you to examine the record(s) at [*place and address*] on [*date*] at [*time*]. If you are unable to examine the records at that time, please contact this office to make alternative arrangements; or
- The record(s) containing your health information to which you are being given access cannot be copied. We invite you to examine the original record(s) at [*place and address*] on [*date*] at [*time*]. If you are unable to examine the record(s) at that time, please contact this office to make alternative arrangements.

Access to all other records has been denied under section(s) [*give detailed sections*] of the *Health Information Act.*

Model Letter F – Response to Access Request – Denial of All or Part of Record(s) (continued)

Option F.3: Severed Information

Some of the records you requested contain information that is excepted from disclosure under *the Health Information Act*. We have severed the excepted information so that we could disclose to you the remaining information in the records.

The severed information is excepted from disclosure under sections [*provide section numbers and descriptors*] of the *Act*. The detailed sections supporting the excising of particular information is [*provided in the attached list or indicated on the face of each record*].

Under section 73 of the *Health Information Act*, you may ask the Information and Privacy Commissioner to review the decision not to disclose information that you requested. You have 60 days from the receipt of this notice to request a review by writing to:

Information and Privacy Commissioner
410, 9925 – 109 Street
Edmonton, Alberta, T5K 2J8.

OR

We are disclosing (all or part of the particular records) outside the provisions of the *Health Information Act* and a copy of these is enclosed.

[***If fees are to be charged, reference should be made to the options for additional wording in Model Letter E.***]

Under section 73 of the *Health Information Act*, you may ask the Information and Privacy Commissioner to review the decision that the records that you requested are excluded from the scope of the *Act*. You have 60 days from the receipt of this notice to request a review by writing to:

Information and Privacy Commissioner
410, 9925 – 109 Street
Edmonton, Alberta, T5K 2J8.

Model Letter F – Response to Access Request – Denial of All or Part of Record(s) (continued)

If you wish to request a review, please provide the Office of the Information and Privacy Commissioner with the following information:

1. The reference number quoted at the top of this notice.
2. A copy of this letter.
3. A copy of your original request for information that you sent to [*custodian*].

If you have any questions about this letter, please write or call me at [*telephone number*].

Sincerely,

[*Name*]
[*Title*]

Model Letter G – Response to Access Request – Record Does Not Exist

Purpose: To advise an applicant that a record does not exist.

[*Reference number*]

[*Date*]

[*Applicant's name and address*]

Dear [*Applicant's name*]:

Re: Health Information Act
[*Request under Consideration*]

I am writing about your request of [*date*] for access to information under the *Health Information Act*.

I regret to inform you that a search by [*name of custodian*] has failed to retrieve any records relating to the subject of your request. [*Outline all steps taken to locate records and, if the records have been destroyed, provide information, if possible, as to when and under what authority this was done.*]

Under section 73 of the *Health Information Act*, you may ask the Information and Privacy Commissioner to review the finding that records pertinent to the request [*could not be located or have been destroyed*]. You have 60 days from the date of this notice to request a review by writing to:

Information and Privacy Commissioner
410, 9925 – 109 Street
Edmonton, Alberta, T5K 2J8.

Model Letter G – Response to Access Request – Record Does Not Exist (continued)

If you wish to request a review, please provide the Office of the Information and Privacy Commissioner with the following information:

1. The reference number quoted at the top of this notice.
2. A copy of this letter.
3. A copy of your original request for information that you sent to [*name of custodian*].

If you have any questions about this letter, please write or call me at [*telephone number*].

Sincerely,

[*Name*]
[*Title*]

Model Letter H – Acknowledgment of Receipt of Correction or Amendment Request

Purpose: *To acknowledge receipt of the applicant's request to correct his or her personal information.*

[*Reference number*]

[*Date*]

[*Applicant's name and address*]

Dear [*Applicant's name*]:

Re: Health Information Act
[*Request for Correction or Amendment under Consideration*]

Your request for correction or amendment of health information [*describe requested correction or amendment*] under the *Health Information Act* [the *Act*] was received by [*name of custodian*] on [*date*].

We will respond to your request by [*date*], or sooner if possible.

If you have any questions, please write to me or call me at [*telephone number*].

Sincerely,

[*Name*]
[*Title*]

Model Letter H.1 – Notice of Processing a Request for Correction or Amendment under the *FOIP Act*

Purpose:	*To acknowledge receipt of the applicant's request to correct his or her health information and to give notice that all or part of the request will be processed under the FOIP Act.*

[*Reference number*]

[*Date*]

[*Applicant's name and address*]

Dear [*Applicant's name*]:

Re: Health Information Act
[*Request for Correction or Amendment under Consideration*]

Your request for correction or amendment of health information [*describe requested correction or amendment*] under the *Health Information Act* [the *Act*] was received by [*name of custodian*] on [*date*].

Some (or all) of the records you requested to be amended contain information to which the *Freedom of Information and Protection of Privacy (FOIP) Act* applies. The request for correction or amendment of those records is deemed to be a request under Section 35 of the *FOIP Act* and that *Act* applies to the processing of your (or that part of your) request.

Please see the attached letter related to your (or that part of your) request [*attach a letter acknowledging receipt of request for correction under the FOIP Act – use Model Letter R from Appendix 3 – FOIP Guidelines and Practices (2000)*].

If you have any questions, please write to me or call me at [*telephone number*].

Sincerely,

[*Name*]
[*Title*]

Model Letter I – Notification Concerning a Request for Correction or Amendment

Purpose: To advise an individual whether or not a request for correction or amendment has been agreed to and other parties have been notified and, where it has not, what the applicant's options are.

[*Reference number*]

[*Date*]

[*Applicant's name and address*]

Dear [*Applicant's name*]:

Re: Health Information Act
[*Request for Correction or Amendment under Consideration*]

Option I.1: Correction or Amendment Agreed To

Your request for a correction or amendment of [*error or omission*] has been agreed to by [*name of custodian*] and your record has been corrected or amended as you requested.

A copy of your new record incorporating the correction or amendment accompanies this notice [*or you can inspect the corrected or amended record at – name and address of appropriate office*].

The following persons, [*name persons*], to which the information has been disclosed over the last year have been informed of the facts of [*the correction or amendment*] and requested to amend their files to reflect this information.

Option I.2: Correction Refused

Your request for a correction or amendment of [*error or omission*] has been refused by [*name of custodian*], you may either:

(a) Ask for a review of this decision by the Information and Privacy Commissioner under section 73 of the Act;

OR

Model Letter I – Notification Concerning a Request for Correction or Annotation (continued)

(b) Submit within 30 days of receiving this notice a statement of disagreement to [*the custodian*] setting out in 500 words or less the requested correction or amendment and your reasons for disagreeing with this decision.

[*If applicant submits a statement of disagreement*] Your statement of disagreement will be attached to the record that is the subject of the requested correction or amendment and will be provided to any person to whom [*name of custodian*] has disclosed the record in the year prior to your request.

[*In the case of refusal*] You may request the Information and Privacy Commissioner to review our decision to refuse to correct or amend your health information. The *Act* allows you 60 days from the date you receive this notice to request a review by writing to:

Information and Privacy Commissioner
410, 9925 – 109 Street
Edmonton, Alberta, T5K 2J8.

If you wish to request a review, please provide the Office of the Information and Privacy Commissioner with the following information:

1. The reference number quoted at the top of this notice.
2. A copy of this letter.
3. A copy of your original request for correction which you sent to [*name of custodian*].

If you have any questions, please write to me or call me at [*telephone number*].

Sincerely,

[*Name*]
[*Title*]

Model Letter J – Notice to Persons in Receipt of Health Information

Purpose: *To advise persons who have received health information that a correction or amendment has been made or that a statement of disagreement has been submitted.*

[*Reference number*]

[*Date*]

[*Name of person and address*]

Dear [*Name of official*]:

Option J.1: Correction or Amendment Made

On [*date*], [*name of custodian*] disclosed to you information concerning [*name of individual requesting correction or amendment*]. This information has [*been corrected or amended and a copy of the corrected record is attached*]. Section 13(3)(c) of the *Health Information Act* requires that we notify you of this correction. Please amend your records or link the correction or amendment to them in order to ensure that they contain this new information.

Option J.2: Statement of Disagreement Submitted

On [*date*], [*name of custodian*] disclosed to you information concerning [*name of individual requesting correction or amendment*]. This information has not been corrected or amended but [*name of individual*] has submitted a statement of disagreement under section 14(1)(b) of the *Health Information Act*. Section 14(3) of that *Act* requires that we provide a copy of this statement of disagreement to you to attach to the information that was disclosed to you (see attached statement).

Sincerely,

[*Name*]
[*Title*]

Model Letter K– Notice Agreeing to Make a Correction or Amendment and Dispensing with Notification of Persons About a Correction or Amendment

Purpose: *To advise an applicant that a request for correction or amendment has been agreed to and to obtain the applicant's consent to dispense with notifying other persons about the correction or amendment.*

[Reference number]

[Date]

[Applicant's name and address]

Dear [Applicant's name]:

Re: Health Information Act
[Request for Correction or Amendment under Consideration]

Your request for a correction or amendment of [error or omission] has been agreed to by [name of custodian] and your record has been corrected or amended as you requested. The record containing the information that you requested to be corrected or amended has been disclosed over the last year to the following persons [name persons]:

Since [name of custodian] believes that you will not be harmed if the above persons are not notified about the correction or amendment, we are asking for your consent to dispense with notifying those persons under section 13(4) of the *Health Information Act*.

Please sign and return the attached form, indicating whether you consent to dispensing with notification.

If you have any questions, please write to me or call me at [telephone number].

Sincerely,

[Name]
[Title]

Model Letter K– Notice Agreeing to Make a Correction or Amendment and Dispensing with Notification of Persons About a Correction or Amendment (Continued)

Consent to Dispense with Notification About a Correction or Amendment

I, [Name of Applicant] consent to [Name of Custodian] not notifying the persons to which my health information has been disclosed during the year prior to my request for a correction or amendment, dated [date of request], that my health information has been corrected or amended.

Dated this [day] of [month], [year]

Expiry date [day] of [month], [year]

[Signature of Applicant]

[Name of Applicant]

[Witness Signature] [Witness Name]

APPENDIX 3

Responsibilities of Custodians

and

Health Information Act Implementation Checklist

Appendix 3
Responsibilities of Custodians in Administering the *Health Information Act*

In preparing to implement the *Act*, each custodian should establish internal processes and procedures suited to the organization's size, structure, specific circumstances and anticipated workload. A custodian's responsibilities under the *Act* include:

- receiving and responding to requests for health information, meeting the duty to assist applicants and collecting any fees as set out in the *Act* (sections 7-10, 12, 15, 17 and 67);
- deciding what information will be released and what information will be excepted from disclosure under the legislation (section 11);
- receiving and responding to requests for correction or amendment (sections 13-15);
- fulfilling the various duties of the custodian relating to the collection, use and disclosure of health information, including the rules regarding the least amount of information and the highest degree of anonymity (sections 18-72);
- responding to the Information and Privacy Commissioner to resolve reviews and complaints under the *Act* (sections 73-82, 84, 85); and
- assisting the public by designating one or more individuals to be responsible for the implementation and administration of the *Act* and making available any policies or procedures regarding the implementation of the *Act* (sections 62 and 63).

Health Information Act Implementation Checklist

The following issues and tasks should be addressed by a custodian before the *Act* comes into effect. Although they are arranged for the most part in relative priority, many of these tasks can be completed simultaneously during the period prior to proclamation.

1. Establish the structure necessary to administer the Health Information Act

- **Designate a responsible person(s)**

Custodians have a number of responsibilities and requirements related to the implementation, administration and operation of the *Health Information Act*. Regardless of the size and structure of the custodian, fulfilling these responsibilities will require clear lines of responsibility and coordination within each organization.

Section 62 of the *Act* requires each custodian to identify an individual who will be responsible for implementing the *Act* and the regulations made under it. This individual is also responsible for ensuring that the necessary *Health Information Act* related policies and procedures are established and followed.

The *Act* provides flexibility for custodians. If the custodian organization is large or decentralized, it may choose to identify individuals responsible for the *Act* on a site by site or geographic basis, rather than having one person responsible for full implementation. Designated individuals may be employees or agents of the custodian. "Best practices" point to the importance of having only one individual designated, if possible, with support from site or area/program contacts as necessary. The designated individual should have access to senior staff and decision makers and the necessary resources and support.

A single individual or agent may represent several custodians in a clinic or facility setting or in instances where custodians do not have the capacity to administer the *Act*. These arrangements should be formalized to ensure that the scope of responsibility is clear. As in other areas of the *Act*, the custodian remains ultimately responsible for the actions of their agents.

- **Forecast volume of requests**

Custodians should attempt to forecast the volume of requests for health information they may receive under the *Act* and prepare an implementation plan with this forecast in mind.

In most instances, custodians are already helping people to access records containing their health information. Current access may be granted under the *FOIP Act*, under practice guidelines based on the Supreme Court of Canada decision in 1992, or under other rules or processes. Current volumes of requests likely reflect factors such as public awareness of the ability to request access to information, the actual or perceived barriers to access, the time it takes to get access to information, and so on. These factors should be considered when preparing forecasts of future volumes of information requests. Once the *Act* is proclaimed, greater public awareness regarding the right of access and fees may result in an increase in the number of requests, but the actual increase is likely to vary for different organizations and parts of the province.

- **Establish an appropriate implementation support team**

Depending on the projected volume of requests, the amount and type of health information collected, used or disclosed, and the size and complexity of the organization, a custodian may wish to establish a team to support the person responsible for implementing the *Act*. In a large organization such as a health authority, the team should likely include senior representatives from the various parts of the organization affected by the *Act* (i.e. those areas that collect, use or disclose health information). It may also include a representative from information technology and systems, information or records management, the legal department and human resources.

Custodians that provide a single health service or work in a clinic will have very different support needs. In these cases, support will be provided primarily by the department.

Regulatory bodies or other support organizations may also support custodians and provide advice in implementing the *Act*. The various support roles will be developed and communicated as early in the implementation process as possible.

- **Identify and communicate with other "affiliated" custodians**

Under the *Act*, some custodians will have responsibility for other custodians. For example, a regional health authority will have some level of responsibility for subsidiary health corporations, community health councils, other boards, councils, committees or agencies that they create and perhaps hospitals and nursing homes funded to perform services in the region. In these cases, the custodian should identify all the various other custodians they are responsible for as early as possible and take steps to determine how to implement the *Act* for, or with, them.

2. Establish a communications plan

The department of Alberta Health and Wellness is responsible for overall leadership and direction in communicating with the public about implementation of the *Act* and will work with the various custodians to ensure that appropriate information and materials are available.

In addition, each custodian should have an internal and external communication plan in place. The plan should include:

- key messages the custodian wishes to communicate about its responsibilities and activities in implementing the *Act*;
- activities designed to make all the patients, clients, residents, agents, and employees aware that the *Act* applies to the custodian and how the custodian's operations will change to comply with the requirements of the *Act*; and
- any special messages and approaches to communicate with the media and special groups that interact with the custodian.

The department will provide samples of communications templates such as newsletters, brochures, posters and so on to all custodians. Those materials and templates will be developed in consultation with custodians and various organizations. Custodians will be able to use the templates directly or modify them to meet their specific needs, while still maintaining the core content.

3. Establish a training plan and conduct awareness training

Training and awareness sessions will be very important as implementation proceeds. In medium to large organizations, these sessions should begin as soon as possible to ensure that senior management and staff understand the requirements of the *Act*.

In medium to large organizations, the training plan should accommodate a variety of audiences and their requirements including the following:

- site or facility contacts, program contacts and back-up contacts (if required) will require an in-depth knowledge of the procedural and interpretative aspects of the *Act*;
- senior staff will require a general knowledge of the procedural and interpretative aspects of the *Act*, including its impact on the operations of the organization;

- members of the governing authority (e.g. boards) should understand the principles and overall approach of the *Act*, its general requirements and impact on the organization;
- staff who have daily contact with the public must be able to recognize and channel both health information requests and freedom of information (FOIP) requests, if applicable, to the appropriate contact points for response;
- all staff and agents of the custodian should be generally aware of the existence of the *Act*, the name of the person responsible for its implementation and operation in the organization and the basic requirements of the *Act*; and
- specific staff groups, such as human resources staff, those responsible for collecting health information in admitting offices or functions, managers responsible for internal operations and support functions, information systems and information management specialists, legal advisors and others will need a detailed understanding of the *Act* as it relates to their specific area of expertise.

Training and awareness in small offices or organizations will pose different challenges. While the person responsible for the implementation of the *Act* can likely be the centre of knowledge about the *Act* in the short term, others in positions of responsibility and those who interact directly with individual patients clearly need to understand the rules in the *Act*, their implications and the administrative requirements.

Training materials have been produced by the department and training courses were conducted prior to the proclamation date. The training materials are available for custodians to use in their own training programs.

4. Assess the status quo

While it will take time to prepare and distribute all of the necessary materials to fully support and implement all aspects of the *Act* and regulations, the major provisions of the *Act* point to the areas where the impact on the custodian will be the greatest. Custodians can begin to review their current processes for collection and use of health information with the general requirements of the *Act* in mind.

The following is a list of areas where operations may be affected and key questions to ask in a preliminary assessment. Once again, the size and complexity of the organization will directly impact the amount of effort required to consider these areas.

- **Who are the affiliates of the organization?**

  The definition of affiliates in the *Act* includes a custodian's employees and those in a contractual or agency relationship. A list of who, beyond the organization's employees, falls into this definition can be built over time and will be useful as communications and training strategies are developed. Begin thinking about which employees or agents have a role, or set of duties, in the office or organization that requires them to access identifying health information, and whether that access needs to be blanket access, or access only to some information in some circumstances.

- **What are current practices?**

Current practices may need to be revised to reflect the new requirements of the *Act*. While more details on the specific requirements of the *Act* are being developed, current collection, access, use, disclosure, disposition, data matching and security policies and practices need to be identified and understood. While a general sense of these areas can and should be obtained early on in the process, a full "privacy audit" of the organization may be completed over a longer period of time. Each operational area can be explored based on the major components of the *Act*.

Think about these questions:

- **Collection** – What is the current authority for collection of information? Is information collected directly from the individual or from other sources (If another source, why? Under what conditions?) Is information about the collection provided to individuals at the time of collection? Are hidden cameras or other recording devices used to collect health information?
- **Access** – Is individual access to health information possible currently? Under what authority? At what cost? How quickly does the individual obtain access? Would the individual benefit from the current practice continuing, even with the proclamation of the *Act*?
- **Use** – What is the role and mandate of the organization in relation to those purposes listed in Section 27 of the *Act*? Are some of the purposes listed more relevant than others? What amount and type of information is necessary to fulfill those purposes? Is more information collected or used currently than may be necessary?
- **Disclosure** – Where does health information currently go? What amount and type? Under what authority? Do the disclosure sections of the *Act* (sections 35-37) appear to allow this type of disclosure to continue?
- **Disposition** – How and when does health information currently get disposed of in both hard copy and electronic form?
- **Data matching** – Does any data matching or data linking activity currently take place? If so, with whom? Does it occur on a occasional (i.e. batch) basis or does it occur as part of a regular process?
- **Security** – How is health information currently secured in both hard copy and electronic systems? To what extent is access controlled? Is it on a "need to know" basis? How is information that is transmitted or transferred secured?

- **What are the current practices for records management and archives?**

Consider these questions:

- Do the current records and information management systems enable responsible staff to locate and retrieve records containing health information about an individual in an complete, accurate and timely manner? This includes records in all formats including paper-based files, electronic patient files, electronic databases and other media. It also includes all types of files that may contain health information about an individual including the patient medical record, material waiting to be transcribed or entered into the patient record, information about the patient that may exist in other places (e.g. subject-based files on specific diseases or procedures, etc.).

  - What amount and type (i.e. diagnostic treatment and care, registration and health service provider) of health information exists in the organization, in what format and where? It may also be helpful to know whether the three types of information always exist together or whether there are instances where one or more types exist apart from the others. This distinction will make it easier to determine which rules apply to which information.
  - Which records in the custody or control of the organization will be exempt from the *Health Information Act*, or otherwise covered by another *Act*, such as the *FOIP Act*?
  - What are the current records retention and disposition practices (i.e. how long are the various types of health information records kept for) of the organization and what is the basis for current practice?
  - What health information has been, or will be, provided for archival storage? If any information is stored in archives, it is important to be clear on who manages those records currently and under what rules.

- **Are Personal Health Numbers collected and used?**

  If the Personal Health Numbers (PHNs) of individuals are collected by the organization, what are they used for? Are they used only for the purposes for which they were collected, or for other purposes as well?

- **What legal authority is in place?**

  What legal authority does the organization currently rely on to support existing collection, use and disclosure practices? Any one of a number of existing statutes and/or regulations could be relevant to a custodian's operations. The *Health Information Act* allows many existing practices to continue if they are fully authorized by an existing statute or regulation.

- **What policies are in place for consent?**

  What are the organization's current practices, requirements and reliance on consent for collection, use and disclosure of health information? If consent is required, is it "informed" consent provided in written form? Or, is verbal or implied consent also acceptable? How is consent generally administered in the organization?

- **What projects and activities will be affected by the new Act?**

  Are there any new information systems, administrative practices or data matching plans currently in development that are likely to come into effect just prior to or after the *Health Information Act* comes into effect? If so, those involved in these projects need to understand the new requirements of the *Act* and the impact those requirements will have on their projects.

- **How are the various levels of anonymity determined and achieved?**

  As the *Act* requires custodians to collect, use or disclose health information at the highest level of anonymity possible to achieve the intended authorized purpose, an organization must have some ability to create or view information at various levels of anonymity. What is the current level of knowledge and ability within the organization to transform information so it can be provided at different levels of anonymity? Is the organization able to acquire those services from another source?

- **What contracts will be affected?**

  Contractors providing services, including information services, to the custodian will be constrained in many areas under the *Act*. The terms of the contract or agreement between the parties will be important to establish roles and responsibilities relative to the various dimensions addressed in the *Act*. Existing contracting practices and contractor obligations need to be reviewed to determine if health information held by the contractor can be accessed on behalf of the individual and that the contractor is subject to the necessary and appropriate privacy and security constraints. Existing contracts that may be of issue need to be highlighted for further review.

5. Develop procedures for tracking and responding to health information requests

The *Health Information Act* sets out time limits for processing and responding to requests for health information and corrections, calculating fees and defending decisions and actions if there is an appeal to the Information and Privacy Commissioner. The person responsible for implementing the *Act* needs to develop effective procedures to ensure that these time limits can be met. The procedures should reflect the overall approach taken by the custodian to implement the *Act*.

The nature and details of these procedures will vary among custodians, depending on the size, complexity and administrative structure of the organization. However, the procedures and assigned responsibilities should generally address:

- receiving requests for health information and corrections;
- creating a request file;
- accepting verbal and written requests;
- locating and retrieving health information records;
- administering fees;
- applying exceptions to the right of access;
- severing records;
- responding to applicants;
- explaining terms, codes and abbreviations used in the records;
- closing the request file;
- preparing for a review by the Office of the Information and Privacy Commissioner; and
- determining what information will be available without a request under the *Health Information Act*.

More detailed guidance on these procedural matters will be addressed in the communications, policy and training materials to be provided prior to proclamation.

6. Develop a plan to ensure compliance with the privacy provisions of the Act

The person responsible for implementing the *Act* needs to ensure that the business practices of the organization are reviewed and adjusted to meet the requirements of the *Act*. New practices should be based on the provisions in the *Act*, on regulations that will be developed under the *Act*, and on policies and procedures issued by the department.

Business practices involving the collection, use, disclosure, disposition and security of health information will vary among custodians depending on the size, complexity and administrative structure of the organization. However, policies, practices and assigned responsibilities should generally address:

- assessing the least amount of information required;
- assessing the highest degree of anonymity of information required and how information can be transformed;
- ensuring that the expressed wishes of individuals are considered;
- disclosing individually identifying diagnostic, treatment and care information by electronic means;
- ensuring adequate safeguards;
- ensuring accuracy of information;
- providing notification at disclosure of data matching and authority/purpose statements;
- providing notations of disclosure of records of individually identifying diagnostic, treatment and care information;
- establishing procedures for authenticating the identity of individuals and recipients;
- providing for compulsory disclosure and appeals;
- establishing research review processes and agreements;
- establishing policies for Personal Health Numbers ;
- defining employee and agent authority regarding identifying health information;
- establishing the obligations of gatekeepers; and
- assessing privacy impact of new systems, practices and data matching proposals.

Appendix 3
Health Information Act Implementation Checklist

1. **Establish the structure necessary to administer the *Health Information Act***

- Designate a responsible person(s)
- Forecast volume of requests
- Establish an appropriate implementation support team
- Identify and communicate with other "affiliated" custodians (e.g. subsidiary health corporations, community health councils, etc. for which a regional health authority has responsibility)

2. **Establish a communications plan**

3. **Establish a training plan and conduct awareness training**

- Medium to large organizations
- Small offices and organizations

4. **Assess the status quo**

- Who are affiliates (employees/agents) and what are their duties?
- What are current collection, access, use, disclosure, disposition, data matching and security policies and practices?
- Review records management and archives practices
  - What amount and type of health information exists?
  - Will some records be exempt from the *Health Information Act* or subject to other *Acts*?
  - Current records retention/disposition practices and basis?
  - Any information provided for archival storage – how is it managed?
- If the Personal Health Number is collected, how is it used?
- What is the legal authority for current practices?
- Current reliance on consent?
- New systems, practices or data matching plans in development?
- Anonymity transformation knowledge and ability?
- Contracting practices/contractor obligations?

5. **Develop procedures for tracking and responding to access requests**

- Receipt of health information and correction requests
- Creation of a request file
- Acceptance of verbal vrs written requests
- Locating and retrieving health information records
- Fee administration
- Application of exceptions to the right of access
- Severing records
- Responding to applicants
- Explanation of terms, codes and abbreviations used in the records

- Closure of a request file
- Preparation for review by the Information and Privacy Commissioner
- Determine what information will be available without a request under the *Health Information Act*

6. Develop a plan to ensure compliance with the privacy provisions of the *Act*

- Least amount of information assessment
- Highest degree of anonymity assessment and transformation
- Express wishes administration
- Disclosure by electronic means
- Adequate safeguards
- Ensuring accuracy
- Notification at disclosure
- Notation of disclosure
- Recipient authentication practices and policies
- Compulsory disclosure and appeals
- Research review processes and agreements
- Personal Health Number use administration
- Defining employee and agent authority re identifying health information
- Gatekeeper obligations
- Assessing privacy re: new systems, practices and data matching proposals

APPENDIX 4

Components for Agreements
Under the
Health Information Act

Appendix 4
Components for Agreement with Information Manager

(Section 66(2) of the *Health Information Act*)

Note that this document is intended to be used only as a checklist of components for an agreement with an Information Manager under section 66(2). It does not constitute a precedent or legal advice. Parties to the agreement need to determine what provisions should be in the agreement, giving consideration to their relationship and the tasks that the Information Manager will perform.

INTRODUCTORY MATTERS

1. Names of parties.
2. Authority to enter agreement – section 66(2) of the *Health Information Act*.
3. Duration of agreement.

SERVICES TO BE PROVIDED

4. Description of services to be provided by Information Manager including any transformation of information services.
5. Description of health information that is the subject of the agreement.
6. Financial arrangements – could be attached as a schedule.

RESPONSIBILITIES OF INFORMATION MANAGER

7. The Information Manager must comply with the *Health Information Act*, the regulations under the *Act* and the terms and conditions of the agreement with respect to the information disclosed to it by the custodian.
8. The Information Manager must use the information only for the purposes specified in the agreement, unless the custodian has authorized additional uses in writing.
9. The Information Manager may disclose health information to the custodian that provided the information to the Information Manager.
10. The Information Manager may disclose health information to a custodian other than the custodian that provided the information to the Information Manager only if the Information Manager has been appointed as an affiliate of that (or those) other custodian(s) and only as authorized by the custodian, according to disclosure rules and processes as outlined in the *Act*.

    Note: An Information Manager that is appointed as an affiliate of other custodians who are participating in a database managed by the Information Manager may disclose health information to those participating custodians but in order to satisfy section 58 of *HIA*, the custodian must:

    - **minimize the health information that the custodian contributes to the database;**

- **implement security precautions to restrict access to information in the database by participating custodians or structure the database so that participating custodians do not have direct access to it;**
- **obtain the consent of the individuals who are the subjects of the health information in the database; and**
- **obtain the advice and recommendations of the Information and Privacy Commissioner before the database is operational.**

11. The Information Manager must comply with the terms and conditions relating to the type of records storage media, the length of time the information is to be retained and the method of disposition to be used in destroying or archiving the information.
12. The Information Manager and their employees must only modify the information in accordance with the terms of the agreement.
13. The Information Manager must protect the information against such risks as unauthorized access, use, disclosure, destruction, or alteration and limit "access" to the information only to those employees who have a need to know. The Information Manager must comply with the requirements of section 60 of the *Health Information Act* and section 8 of the Health Information Regulation relating to the security of health information (could attach a copy of the Regulation as a schedule to the Agreement).
14. The Information Manager must notify the custodian in writing immediately if the Information Manager or their employees become aware that any of the conditions set out in the agreement have been breached.
15. The recorded information held by the Information Manager is under the custody or control of the custodian for the purposes of the *Health Information Act*.
16. Requests by individuals, or their authorized representatives, to access information held by the Information Manager will be directed to and handled by the custodian, but the Information Manager will have a specified role in the retrieval of the requested information for the custodian. (Timelines and costs for retrieval should be indicated and in keeping with the provisions of the Act and Regulations. The timeline for retrieving the requested information and providing it to the custodian should be relatively short i.e. 4-5 days to fit within the 30 day timeline in the Act).

INDEMNITY

17. The Information Manager must agree to be fully and solely responsible for the actions of its employees, agents, consultants and other persons respecting the use or disclosure of the information and for any unauthorized disclosure or use of the information as a result of carrying out the Agreement, regardless of the cause (including, but not limited to, negligence, misfeasance, malfeasance, accident or neglect) during the term of the Agreement or after the expiration or earlier termination of the Agreement.
18. The Information Manager must agree to hold the custodian harmless from any third party claims, demands or actions for which the Information Manager is legally responsible, including those arising out of negligence, willful harm or crimes by the Information Manager or its employees or agents.
19. The Information Manager must agree to indemnify the custodian for any and all costs or expenses paid or incurred by the custodian as a result of any breach of any term or condition

of this Agreement or contravention of the *Act* or regulations or arising out of any disclosure by the Information Manager of the health information that is subject to this Agreement in any manner contrary to the Agreement. Such indemnification will survive the termination of the Agreement.

20. The custodian is not responsible for any bodily or personal injury or property damage or business losses that may be suffered or sustained by the Information Manager, its employees or agents in the performance of the Agreement.

TERMINATION

21. The agreement may be terminated by either party under certain conditions prior to its completion.
22. In the event the agreement is breached and/or health information is disclosed or used in contravention of the terms and conditions of the agreement or the *Act* or regulations, the agreement may be immediately cancelled by the custodian and the Information Manager may be found guilty of an offence under section 107 of the *Act*.

GENERAL PROVISIONS

23. The agreement may be amended or varied in writing with the mutual agreement of the parties.
24. The parties must each designate an individual for responsibility for the agreement, notices and communications (include the contact information for the designated individuals).

EXECUTION

25. The agreement must be signed by officers or other officials of the parties who have authority from the parties to sign such an agreement.

Appendix 4
Components for a Research Agreement

(Section 54 of the *Health Information Act*)

Note that this document is intended for use only as a checklist of components for a Research Agreement under Section 54. It does not constitute a precedent or legal advice. Parties to the agreement need to determine what provisions should be in such an agreement, giving consideration to their relationship and the tasks that the researcher will perform.

Where the researcher is an affiliate of the custodian (employee or physician with privileges), the agreement may need to be modified depending upon the nature of the relationship between the custodian and the affiliate.

Introductory Matters

1. Names of parties to the agreement.
2. Identification of lead researcher who is bound by this agreement.
3. Statement that the researcher has applied to the custodian for disclosure of health information for the research purposes [as listed in Schedule A – application for disclosure of health information to be used in research including the research purpose(s)] (section 52).
4. Description of Research Project (reference to Schedule B - full research proposal or summary of the research proposal).
5. Statement that the designated ethics committee is satisfied that the researcher has met the requirements of section 50 [the ethics committee must be designated by the Minister in the Health Information Act Designation Regulation]. Include the name of the designated ethics committee that reviewed the proposed research project and when approval was granted.
6. Statement that the custodian has decided to disclose the health information applied for to the researcher (section 53).
7. Statement that the researcher will or has obtain(ed) the consents of the individual subjects prior to disclosure of their health information, if obtaining consents was recommended by the ethics committee (section 50(1)(a)).
8. Duration of Research Project and duration of the Research Agreement. [Could add an ability to extend the time limits with consent of the custodian].

Responsibilities of Researcher

9. The researcher agrees to comply with:
   - the *Health Information Act* and all regulations under that *Act* (section 54(1)(a)(i));
   - any conditions imposed by the custodian relating to the use, protection, disclosure, return or disposal of the health information (section 54(1)(a)(ii)); and

- any requirements of custodian to provide safeguards against the identification, direct or indirect, of an individual who is the subject of the health information (section 54(1)(a)(iii)).

10. The researcher understands that if he/she knowingly breaches the terms and conditions of the research agreement, he/she is guilty of an offence and liable to a fine of up to $50,000 (section 107(3) and (6)).

Responsibilities of Custodian

11. The custodian agrees to disclose the research information or data in a specific format at specific time(s) [reference to Schedule C – specifics of the research information (data sources/elements) and any other information to be disclosed].

12. The custodian agrees to obtain consents to contact the individuals who are the subject of the information to obtain additional data. [Alternatively, this clause could bar the researcher from any further contact, depending on the nature of the research] (section 55 or section 54(1)(d)).

Restrictions on Use and Disclosure of Health Information

13. The researcher agrees to only use the research information (data sources/elements) and any other information disclosed by the custodian [reference Schedule C] for the purposes as identified in Schedule A (section 54(1)(b)).
14. The researcher agrees not to use or disclose the information for any subsequent or other purposes not identified in Schedule A without the prior written approval of the custodian [and/or the consent of the individual who is the subject of the information, if required by the custodian]. The custodian may arbitrarily withhold consent for subsequent uses (section 54(1)(b)).
15. The researcher agrees to disclose information only to individuals working with the researcher on the research project (include names or positions of individuals working with researchers).
16. The researcher agrees to ensure that all individuals on the research team that have access to the information are complying with the *Health Information Act* and regulations and with any conditions and/or requirements imposed on the researcher by the custodian (section 54(1)(a)).

Publication of Results

17. The researcher agrees that no identifying information or information that could be manipulated to identify any individual will be published (section 54(1)(c)).
18. The researcher agrees to provide the custodian with the proposed report (or publication) of the results of the research for the custodian's review and the custodian agrees to acknowledge its receipt. The report (or publication of results) must include a statement that some of the information used in this study was provided by the custodian and the custodian expresses no opinion on the interpretations and conclusions in this publication.

Requirements to Safeguard Data

19. The researcher agrees to adequately safeguard the confidentiality and security of the information obtained from the custodian [Depending on the nature of the research and the

data management/manipulation that the researcher will be undertaking, specific requirements for safeguards could be added or referenced in a separate Schedule, including physical, technical, administrative and other security safeguards]. The researcher also agrees to safeguard the privacy of the individuals who are the subjects of the information by ensuring that the individuals who are the subjects of the information cannot be identified, directly or indirectly (section 54(1)(a)(ii) and (iii)).

20. The researcher agrees to report to the custodian any breaches of confidentiality and/or security respecting the information; and to take steps to both remedy the breach and prevent a similar occurrence in the future (section 54(1)(a)(ii) and (iii)).
21. The researcher agrees to allow the custodian to access or inspect the researcher's premises to confirm that the researcher is complying with the *Act* and regulations, any imposed conditions on use, protection, disclosure, return or disposal of the information and any requirements related to the provision of security safeguards (section 54(1)(e)).
22. The researcher agrees to dispose of the information after the research has been completed (set out time period for disposal) by destroying it (indicate method(s) of destruction for both paper and electronic information and electronic storage devices) or by returning it to custodian (set out time period for return).

Financial Arrangements

23. The researcher agrees to pay the custodian the amount of x$, as detailed in Schedule C [which gives details the costs of the researcher [could include cost of information preparation, transmission, copying, and/or obtaining consents] (section 54(3)). Note that these provisions may not apply to sponsored research – a separate agreement with the sponsor will cover the financial arrangements.

Termination

24. In the event the agreement is breached and/or health information is disclosed or used in contravention of the terms and conditions of the agreement or the *Act* or the regulations, the agreement may be immediately cancelled by the custodian, the research privileges of the researcher may be withdrawn, all research information will need to be returned to the custodian and the researcher may be found guilty of an offence under section 107 of the *Act*.
25. The agreement may be terminated by either party under certain conditions prior to its completion.

Indemnity

26. The researcher agrees to hold the custodian harmless from any third party claims, demands or actions for which the researcher is legally responsible, including those arising out of negligence, willful harm or crimes by the researcher (or its employees or agents, if any).
27. The researcher agrees to indemnify the custodian for any and all costs or expenses paid or incurred by the custodian as a result of any breach of any term or condition of this Agreement or contravention of the *Act* or a regulation under the *Act* or arising out of any unauthorized disclosure by the researcher of the health information that is subject to this

Agreement in any manner contrary to the Agreement. Such indemnification will survive the termination of the Agreement.

28. The custodian is not responsible for any bodily or personal injury or property damage or business losses that may be suffered or sustained by the researcher (or its employees or agents, if any) in the performance of the Agreement.
29. The researcher has no recourse against the custodian for any loss or damage arising from the researcher's interpretation or analysis of the information received from the custodian or from the conclusions reached by the researcher. The researcher has no recourse against the custodian for any loss or damage arising from any advice provided by the custodian about the research information.

Where the researcher is an affiliate of the custodian (employee or physician with privileges), the indemnity provisions may need to be modified or deleted depending upon the nature of the affiliate's relationship to the custodian.

Termination of Agreement

30. Statement of the conditions under which the custodian can terminate the agreement, including retention, disposition or return of the information if the agreement is terminated prior to the completion of the research. In some cases, data must be retained for a fixed period (e.g. 7 to 15 years).
31. Statement of the conditions under which the researcher can terminate the agreement prior to the completion of the research, including the responsibility to inform the custodian to cease information disclosure [method of notifying custodian, time periods, etc.].

Other General Provisions

32. The researcher agrees that the consent of the custodian has been obtained prior to the transfer of the agreement to another person. Consent may be arbitrarily withheld in the discretion of the custodian. Successors must be bound by the terms and conditions of the agreement.

Note that if the research agreement is with an individual researcher rather than a corporate entity, the agreement should not be transferable.

33. For any required notices (regarding publication, termination, etc.) under the agreement, the contact information of designated officials of the parties should be listed
34. Provide for the signatures of officials who are authorized by the parties to sign the agreement.
35. Include any other legally required provisions.

INDEX

A

- AADAC 3, 11, 15
- abandonment of a request 55
- ABC Benefits Corporation 15, 163, 173
- absence of consent 112, 198
- abstracting 137
- abuse of the right of access 40
- access controls 118, 119, 176, 128, 285, 294, 303
- access is denied 39
- access request 25, 28, 29, 34, 56, 57, 58, 88, 215, 278, 272, 279, 280, 281, 285, 307
- acknowledging a request 42, 99
- acupuncturists 181
- advice 82, 84
  - advice to Minister or RHAs 75
  - Executive Council 62, 70-73
  - IPC advice 252, 262, 264
  - legal advice 50, 101, 228
  - RHA/Provincial Health Board 74
- affiliate 15
  - responsible affiliate 122, 250, 252-254
- aggregate health information 107, 124, 157-158, 177, 193-194
- Alberta Alcohol and Drug Abuse Commission (AADAC) 3, 11, 15
- Alberta Cancer Board 5, 7, 11, 14, 74, 112, 135, 145, 161, 184, 201, 220-223, 291, 310-311
- *Alberta Evidence Act* 14, 87, 168, 203, 237
- Alberta Health and Wellness 2, 135, 145, 201, 251
- *Alberta Health Care Insurance Act* 10, 11, 208, 220, 310-315, 319
- Alberta Health Care Insurance Plan 3, 4, 11, 14, 163, 166, 183
- Alberta Heritage Foundation for Medical Research 223
- Alberta Innovation and Science 284, 286
- Alberta Mental Health Board 5, 6, 7, 98, 112, 161, 220, 221, 222, 291
- Alberta We//net 143-146
- *Alcohol and Drug Abuse Act* 11, 321
- all methods of communication 119
- ambulance attendants 3, 11, 162
- *Ambulance Services Act* 3, 11, 15, 123, 162, 173, 218, 239
  - Confidentiality Regulation 11
- anonymity 9, 106, 107-108, 129, 136, 157, 177, 178, 182, 193, 200, 220, 221, 250
- anonymity transformation 109, 136, 138, 139
- anonymous information 4, 136
- applicant 29
- appropriate in the circumstances 68
- archives 219
- Attorney General 162, 266
- audiovisual recordings 16, 26, 307
- audit 7, 76, 134, 161, 168, 182, 183, 203, 273, 298, 302, 304
  - IPC 262-263, 278
- audit trails 119, 122, 132-133, 285, 292, 293
- Australia Information Security Policy 121
- authorization and authentication 304
- authorized representative 28-29, 56, 171, 172, 211
- available to the public 167-168

B

- background facts 84
- back-up procedure, see disaster recovery
- Billing Practice Advisory Committee 14
- Breast Cancer Screening Program 10, 144
- British Standard BS 7799: 1995 – Code of Practice for Information Security Management 121
- business arrangements relating to the payment of the health services provider's accounts 13
- business card information 23

C

- Cabinet 70, 71, 82, 83, 84, 86, 274
- Canadian Institute for Health Information 141-143
- Canadian Institutes of Health Research 224
- Canadian Organization for the Advancement of Computers in Health (COACH) 121, 301-302
- *Cancer Programs Act* 14, 19, 74, 184, 307, 310-311
- cellular phone 119, 300, 303
- *Child Welfare Act* 30, 213, 306, 307-309, 311, 316, 321, 328, 336
- chiropractors 14
- CIHI 141-143
- clarifying a request 42, 46, 99
- COACH 121, 301, 302
- collecting a debt 218
- collection chart 174-175
- College of Physicians and Surgeons of Alberta 13, 182, 214, 223
- commercial marketing 9, 177, 216
- committee 14
- communications plan 254
- communications security 118, 303
- community health councils 254
- computer 33, 108, 118, 138, 146, 158, 178, 194, 228, 287, 288
  - based forms 297, 298, 169, 297-298
  - database 6, 110
  - network 109, 110-111,
  - system 6, 109, 117, 119, 146, 229
- confidential source 67-68
- confidentiality 2, 3, 11, 61, 67, 71, 106, 110, 113-114, 116-117, 120, 127, 136, 142, 179, 225-227, 256, 301, 307
  - oath of confidentiality 302
- consent 236

- disclosure of affiliate identity ... 83
- organ donation transplant ... 199
- research ... see section 53(2)(b)
    - ethics committee ... see section 27
    - with consent ... see section 50
    - without consent ... see section 54, 55
- recording device ... 170
    - see also section 23
- revocation of consent ... 200
- with consent
    - commercial purposes ... see section 107(2)
    - disclosure of individually identifying health information ... see section 34
    - electronic means ... see section 59
    - exercise of rights by other persons ... see section 104
- without consent
    - data matching ... see section 1(1)(g)
    - diagnostic, treatment and care information ... see section 35
    - disclosure to Minister of department ... see section 40 and 46
    - disclosure by Minister and department ... see section 39
    - disclosure to other custodians. see section 47
    - health service provider ... see section 37
    - indirect collection ... see section 22
    - information manager ... see section 66
    - maintaining of certain disclosure information ... see section 41
    - registration information ... see section 36
    - storage ... see section 38

consultations
- contingency plans ... 133, 304
- executive ... 70, 72, 82
- PIA ... 125
- request for ... 35, 39, 45, 49-51, 97, 101

continuing care ... 5, 179

contractor .. 27, 67, 76, 123, 180, 181, 203, 288, 304

control ... 26, 256

Controlled Drugs and Substances Act ... 212

Copyright Act (Canada) ... 64

correction ... 3-4, 17, 29, 40, 92-103, 216, 250, 254, 261-263, 265, 267, 272, 292, 307

Court of Queen's Bench of Alberta ... 229, 260, 272, 274

court order ... 8, 28, 204-205, 229, 230

CPSA ... 182, 214, 223

Criminal Code (Canada) ... 208, 212, 316, 321, 330, 335

custodians ... 3
- duty of a custodian ... 8, 33

custody ... 26

custody and control ... 134-135, 148-149, 180, 201, 205, 219, 250, 256, 273, 288, 295-296, 299-301, 307

controlled arena ... 7-9, 11, 140, 250

correcting errors and transmissions ... 279

D

data elements ... 110, 124, 129

data entry ... 157, 304

data linkage ... 124, 148

data matching ... 106, 124, 134-135, 139, 147, 148, 149, 177, 193, 216, 226, 259, 261, 289, 295, 296, 292

data profiling ... 148

decision has been implemented ... 84

decision has been made public ... 84-85

deemed request ... 36, 64, 92, 98

deliberation ... 53, 70-72, 82, 84, 101

deliberative space ... 70

dental mechanics ... 14

dental surgeons ... 14

Dependant Adults Act ... 10, 31, 164

deriving ... 137

destruction of health information ... 115

diagnostic, treatment and care information ... 12

dietary personnel ... 178, 196

direct collection ... 163

directly paid for by the department ... 11

disaster recovery ... 120

discipline proceeding ... 5, 80, 112,180-180, 201, 214, 218

disclosure ... 192
- discretionary ... 5, 8, 205, 208
- notations ... 32, 215, 290
- prohibited by another act ... 89

disclosure chart ... 243-249

disclosure harmful to individual to public safety chart ... 66

disclosure leading to identity chart ... 60

discovery ... 17, 27-28, 204

disposition of personal information ... 122, 133

disposition of recorded health information .. .115, 285

diversion ... 119

document ... 229

donation of a bodily substance ... 11

duty to assist ... 33, 34, 41, 250, 262, 265, 267, 272

duty to protect ... 113, 132, 217, 281, 293, 302, 304

E

eavesdropping ... 119

electronic consent ... 111, 198, 217

electronic means ... 5-6, 8, 106, 109-113, 109, 130, 192, 198, 216-217, 286

electronic records ... 43, 282, 284-285

e-mail ... 44, 100, 110, 119, 127, 282, 284, 285, 303

enactment ... 18, 212

encryption ... 119, 133, 137, 139

encryption algorithms ... 139

- ethics committee ... 5, 9, 112, 132, 149, 181-182, 223-229, 291-292
  - designated ethics committees list ... 223
- exception
  - mandatory ... 39, 53, 60-61, 63, 71, 78, 80, 82, 87
  - discretionary ... 39, 53, 60-62, 64, 70-71, 74, 76, 257
- Executive Council ... 62, 70-72, 82-83
- explicitly ... 67
- expressed wishes of the individual ... 3, 8, 109, 195, 200, 220
- extensions ... 35-36, 96-97, 261-262

F

- family members ... 5, 8, 78, 166, 195, 202, 237
- *Fatality Inquiries Act* ... 19, 63, 213, 308-309, 312, 322, 330
- fax ... 45-47, 110, 119, 133, 219, 257, 294, 300, 303, 304
- fees ... 39, 48, 136, 250
  - assessing ... 37, 41-42, 45-48, 147
  - commissioner review ... 48, 261, 271
  - estimating ... 47
  - excusing ... 46, 48-49
  - no fee ... 93
  - payment of ... 36
  - research ... 229
  - third party ... 28
- fine ... 5, 12, 44, 217, 258, 259
- formal patient ... 32, 164, 197, 211, 213, 268
- *Freedom of Information and Protection of Privacy Act* ... 1, 11, 12, 87, 106, 260, 307, 313, 322, 324
- frivolous or vexatious ... 40
- fully or partially paid for by the department ... 10, 135, 221-222, 291
- fully paid for by the department ... 11
- fundraising ... 9, 177, 216

G

- genetic history ... 166
- Government of Victoria ... 121
- guardian ... 30
- guardian of a minor ... 197

H

- hardware and software ... 33, 108, 18-120, 138, 158, 178, 194, 228, 304
- hardware security ... 303
- harm ... 61
- hazard ... 114
- *Health Disciplines Act* ... 181, 336
- health information ... 26
- Health Information Act coordinator ... 2, 36, 37, 39, 41, 42, 43, 44, 45, 48, 49, 50, 52, 53, 99, 100, 101, 102, 125, 162, 250, 252, 253, 254, 255, 298
- Health Information Regulation ... 4, 6-7, 11, 13-14, 19, 28, 38, 46-48, 109, 113, 115, 147, 177, 186, 198, 200-201, 216-218, 229, 293, 294, 301, 305-306, 313, 318
- *Health Insurance Premiums Act* ... 16, 123, 217, 314, 315, 317, 318
- health profession ... 181
- health professional body ... 12, 13
- health services provider information ... 5, 7, 12, 18, 26, 92, 129, 131, 142, 179, 182, 192, 193, 196, 198, 218, 292
- hepatitis ... 185
- HIV ... 185
- home care ... 145, 161, 179, 196, 201
- Hospital Mental Health Database ... 143
- Hospital Morbidity Database ... 142
- Hospital Privileges Appeal Board ... 14
- *Hospitals Act* ... 14, 15, 18, 19, 162, 180, 182, 252, 307, 308, 311, 312-313, 319, 321, 322, 323, 324, 325, 327, 333, 334
- hospitals not owned or operated by health authorities ... 21
- human resource management ... 7, 161, 182-183
- *Human Tissue Gift Act* ... 87, 199, 311, 331, 332

I

- identity ... 67
- immediate and grave harm ... 64
- imminent danger ... 209
- implementation checklist ... 252-255
- implicitly ... 67, 70, 83
- in confidence ... 67-68
- inaccurate information ... 165
- indirectly paid for by the department ... 11
- information manager ... 110, 115, 121, 139, 136, 140-145, 152
- inspection ... 80, 181, 201, 214, 218
- insurer ... 163
- integrity ... 114, 116-117, 300, 302, 304
- interception ... 119, 300
- Internet ... 110, 168, 193, 300
- *Interpretation Act* ... 18, 36, 98
- Intranet ... 110, 121
- investigation
  - custodian ... 4, 180, 201, 229, 254
  - health professional ... 5, 80, 112, 214, 218
  - IPC ... 1, 6, 127, 252, 259, 260-262, 264-267, 270-273, 278, 287
  - police ... 207

IPC Orders

- IPC Order 96-006 ... 71
- IPC Order 96-015 ... 265
- IPC Order 96-017 ... 62
- IPC Order 96-019 ... 52
- IPC Order 96-020 ... 68
- IPC Order 96-022 ... 44, 100

IPC Order 97-007 71
IPC Order 97-013 67
IPC Order 97-020 .... 51, 94
IPC Order 98-001 271
IPC Order 98-002 34
IPC Order 98-004 30
IPC Order 98-005 51
IPC Order 98-007 63
IPC Order 98-011 281
IPC Order 98-016 52
IPC Order 99-001 71
IPC Order 99-009 280
IPC Order 99-010 67
IPC Order 99-011 .... 53, 101, 270
IPC Order 99-014 .... 34, 271
IPC Order 99-021 .... 54, 279
IPC Order 99-025 204
IPC Order 99-032 26
IPC Order 99-034 63
IPC Order 2000-05 .... 26, 27
IPC Practice Note No 1 61
IPC Practice Note No. 2 .... 53, 268
IPC Practice Note No. 3 273
IPC Practice Note No. 4 265
IPC Practice Note No. 5 268
IPC Practice Note No. 7 272

L

legal authority 169, 297
legal proceedings 17
Lieutenant Governor in Council 250, 260, 274
life-threatening injury 5, 8, 207
limited manner ... 2, 106, 108, 158, 178, 194, 280, 290
line by line review 44, 49, 50, 51, 52
link 94

M

making a reasonable effort 122, 196
Medical Profession Act 13, 218, 278, 335, 336
medical records technician 43, 100
mental health 10, 13, 31, 64
Mental Health Act 19, 32, 164, 165, 182, 197, 211, 213, 268, 308, 309, 311, 312, 313, 321, 322, 325, 332, 333
Mental Health Patient Advocate 14
Mental Health Review Panels 14
midwives 181
Minister of Alberta Health and Wellness 2, 16, 224, 251, 271, 274
Minister of Justice 162, 212
MS Drug Review Panel 14

N

narrowing a request 42
necessary for 160
need to know 8, 108-109, 111, 116, 138, 157, 159, 165, 176, 178, 195, 221-222, 303
non-identifying health information 83, 106-107, 109, 129, 136, 138-140, 140-148, 157-159, 176-177, 179, 182-184, 192-194, 203, 216, 221-222, 259
non-recorded health information 18, 176, 179, 196
non-responsive information 51
not reasonably practicable 165
notification
  collection 168, 277, 288, 297-298
  disclosure 192, 216
  extention 36, 53
nurse 13, 214, 251
  registered psychiatric nurse 181
  licensed practical nurse 181
nursing homes 46, 117, 253, 254, 308
Nursing Homes Act 14, 310, 309, 337
Nursing Homes Operation Regulation 88

O

oath of office 261
offence under the Health Information Act 6, 8, 44, 121, 141, 148-149, 258-259, 266, 272, 280, 313
  police offence 58, 206-208, 266
Office of the Information and Privacy Commissioner
  advice 71
  Officer of the Legislature 209
  ethics review 227
  PIA process 6, 125, 127, 141
  restrictions on disclosure 266
  review process 3, 6, 43, 53, 60, 62, 100-102, 209, 250, 254, 268, 272, 276
  role 125, 261, 278, 252, 258, 260-261, 278
  time extension 35
Officer of the Legislature 8, 209, 252, 260, 262
omission 92
on reasonable grounds 165, 209, 307
opticians 14
optometrists 14, 213
order 205
osteopaths 14
other custodial institutions 202
other public sources 168
out-of-country health services 15

P

paramountcy 18-19, 306, 311
partially paid for by the department 10-11
passwords 117, 119, 197, 303, 304
person in a close personal relationship 202
Personal Directives Act 31, 164, 197, 317, 331
personal health number
  collection 130, 157, 162, 289
  individually identifying 107

  protected ... 4, 9, 163, 176-177, 216
  registration information ... 13
  use ... 186
personal information ... 25
personal service ... 45
Persons with Developmental Disabilities Community Governance Act ... 11, 15
Pharmaceutical Information Network ... 110, 111, 145, 146, 155
Pharmaceutical Profession Act ... 10, 14, 18, 278, 287, 313, 338
Pharmaceutical Profession Regulation ... 278, 187
pharmacies/pharmacists ... 3, 7, 10, 14, 43, 50, 100-101, 109, 111, 121, 145, 169, 178-179, 196, 208, 212, 215, 251, 253, 278, 287
Pharmacy and Drug Act ... 313, 338
physical and environmental security ... 303
physical health ... 64
physical therapists ... 214
physicians ... 14-15, 140, 161, 213, 311
podiatrists ... 14
police investigations ... 5, 8, 206-210, 212-213
policy considerations ... 82
policy development ... 5, 7, 112, 161, 182, 183, 185, 201, 220
pose a threat to public safety ... 6, 49, 64-65, 222
power of attorney ... 31-32, 164, 197, 211
Powers of Attorney Act ... 31
practice review ... 4-5, 80-81, 112, 181, 201, 214, 218
prejudice to tests and audits ... 77
privacy ... 113
privacy impact assessment ... 6, 8, 106, 123, 127-127, 135, 148-149, 221, 226, 256-257, 261, 263, 288, 291-292, 295-296
privacy risk assessment ... 134
procedures ... 80
Protection for Persons in Care Act ... 213, 312, 338
Provincial Archives of Alberta ... 44, 100, 219, 281, 286
provincial health board ... 3, 14, 74, 135, 184, 201, 253, 286, 333, 336
psychiatrist ... 65, 109, 195
public body ... 16, 19, 27, 37, 41, 72, 219, 307
Public Health Act ... 7, 16, 19, 160, 161, 182, 185, 213, 311, 321, 329, 336, 339
public health surveillance ... 5, 7, 112, 161, 185, 201, 220
published in any form ... 168
purpose of collection ... 168

Q

quality assurance committee ... 8, 14, 87, 168, 203
quality assurance record ... 87
quality improvement ... 7, 161, 182, 183

R

readily ascertained ... 107
reasonable expectation ... 208
re-coding ... 137
recommendations ... 71
record ... 16
recording device ... 157, 170, 175
records management policies ... 128, 288
Records Management Regulation (AR 57/95) ... 277, 286-288
records management system ... 279
registration information ... 7, 9, 13, 18, 26, 92, 129, 179, 192, 196, 217, 218, 220, 223, 227, 313
  individually identifying ... 5, 13, 132, 182, 193, 217-208, 220, 223, 292
relates directly to ... 160
repetitious ... 40, 265
request chart ... 58-59
research ... 181, 223
  conducting research ... 7, 112, 161, 181, 206, 226
  data matching ... 135, 149, 296
  disclosure ... 5, 131-132, 192-193, 223, 225, 227, 291-292, 308-309, 311-312
  research proposal ... 223-224, 226
  research agreement ... 227-229, 259
revealing health service provider information chart ... 81
reviewing health information about another individual ... 79
revocation of consent ... 111, 112, 198, 200
right of access ... 28, 46, 279, 285
  abuse of ... 40
  disclosure ... 32
  exceptions ... 60, 88
  exercised by other persons ... 25, 29, 32

S

sections
section 1(1)(iii) ... 135
section 1(1)(iv) ... 135
section 1(1)(vii) ... 135
section 1(1)(a) ... 15, 27, 123, 251-252
section 1(1)(b) ... 29
section 1(1)(c) ... 76, 183, 203
section 1(1)(d) ... 157
section 1(1)(e) ... 260
section 1(1)(f) ... 3, 7, 14, 37, 98, 184, 250, 338
section 1(1)(i) ... 7, 9, 12, 18, 92, 200
section 1(1)(j) ... 182, 223
section 1(1)(k) ... 7, 9, 18, 26, 92
section 1(1)(l) ... 13, 214, 338
section 1(1)(m) ... 10, 17, 108, 158, 160, 178, 180, 194, 211
section 1(1)(n) ... 12, 25, 26, 182, 218
section 1(1)(o) ... 7, 9, 13, 18, 92, 218

section 1(1)(p) 7, 107
section 1(1)(q) 16, 158, 177, 194
section 1(1)(r) 107, 136, 158, 177, 194
section 1(1)(t) 16, 215, 282
section 1(1)(u) 7, 13, 18, 92, 179, 196, 217
section 1(1)(v) 161, 181, 223

section 2 .... 14, 36, 60, 92, 182

section 3(a) 17, 27
section 3(b) 28
section 3(c) 278, 280, 286

section 4 .... 16, 18-19, 37, 63, 87, 199, 254, 265, 289, 306, 307, 323

section 5(2) 4, 199

section 6 .... 16, 186

section 7 .... 133, 292
section 7(1) 26, 28, 29, 37, 38, 44, 88, 215, 323
section 7(2) 51
section 7(3) 28, 36, 46, 48

section 8 .... 11, 28-29, 37, 38, 39, 40, 113, 115, 116, 120, 121, 135, 150, 182, 197, 198, 201, 208, 217, 218, 222, 229, 232-234, 281, 293, 299, 301, 305, 316, 323
section 8(1) 29, 37, 38, 40, 115, 323
section 8(3) 39

section 9 .... 14, 47, 55, 87, 103, 123, 147, 168, 203, 237, 280

section 11(1) 18, 47, 49, 61, 65, 67, 68, 71, 72, 74, 76, 87, 88, 90
section 11(1)(a) 49, 64
section 11(1)(c) 70, 71, 72
section 11(1)(e) 76
section 11(2)(a) 61, 78
section 11(2)(b) 80
section 11(2)(c) 71 82, 84,
section 11(2)(d) 87

section 13 .... 29, 92, 93, 94, 95, 96, 98, 100, 104, 105, 133, 216, 262, 267, 272, 292, 310, 313, 319, 323
section 13(1) 29
section 13(3) 93, 104
section 13(3)(c) 94
section 13(6)(a) 95

section 14 .... 95, 97, 105, 133, 213, 216, 313, 323
section 14(1)(b) 95
section 14(3) 95

section 18 .... 157, 263, 336

section 19 159
section 21 .... 4, 160, 162, 163, 177, 186, 187, 216
section 21(3) 162

section 22 .... 130, 165, 289
section 22(1) 163
section 22(2) 163-168, 263
section 22(3) 19, 63, 130, 168, 169, 296, 297, 308-309, 322

section 23 170
section 23(1) 72

section 24 .... 108, 159

section 25 177

section 26 179

section 27 .... 4, 5, 6, 7, 12, 110-112, 114, 130, 134, 148, 155, 159, 160, 161, 169, 171, 176, 180-185, 187-188, 192-193, 199, 201, 215-216, 220-222, 236, 241, 289, 337

section 28 .... 108, 178

section 29 179

section 30 186

section 31 .... 160, 193

section 32 .... 149, 259

section 33 197

section 34 .... 5, 8, 111, 198, 200, 233, 236, 314
section 34(6) 200

section 35 .... 5, 10, 98, 114, 193, 197-198, 199, 200, 201, 202, 203, 204, 205, 207, 215, 216, 217, 232, 237-238, 240, 308, 309, 323
section 35(1) 5, 215, 217, 238
section 35(1)(i) 28, 204-205
section 35(2) 203
section 35(3) 203

section 36 .... 13, 131, 218, 327, 331

section 37 218

section 38 281

section 39 219

section 41 .... 8, 29, 32, 33, 93, 131, 215, 336

section 42 231
section 42(1) 216
section 42(2) 131, 216

section 43 .... 108, 195, 260, 335

section 44 196

section 45 .... 131, 196-197

section 46 ....8, 131, 135, 220-221, 233-235, 263, 290

section 47 .... 131, 221-222, 291

section 50(1)(a) 224, 227
section 50(1)(b) 181, 188, 225, 226, 227
section 50(2) 226
section 50(3) 227

section 52 227

section 53 .... 5, 227

section 54 .... 5, 131, 227, 228, 229, 259
section 54(1) 228
section 54(3) 228-229

section 55 229

section 56(3) 229
section 56(5) 230
section 56(6) 229

section 57 .... 4, 6 8, 107, 108-109, 113, 129-131, 136, 137, 157-158, 176-178, 192-193, 194, 200, 220, 296
section 57(2) 107
section 57(4). 107

section 58 .... 8, 108, 109, 129, 141, 158, 178, 195, 200, 220
section 58(2) 200, 220

section 59 .... 6, 8, 109, 111, 112, 130, 132, 156, 198, 217, 233, 242, 291
section 59(1) 109
section 59(4). 111
section 59(7) 109, 156, 242

section 60 .... 8, 18, 113, 114, 115, 132, 278, 280, 281, 284, 285, 286, 293, 299, 304
section 60(1) 301
section 60(1)(a) 113
section 60(2) 280, 302

section 61 .... 122, 130, 132, 292

section 62 252
section 62(2) 192

section 63 .... 123, 251, 252, 256

section 65 .... 109, 136, 138, 158, 177, 194

section 66 .... 121, 136, 139, 140, 141, 144, 256, 259

section 67 .... 36, 48, 147, 267
section 67(1) 147
section 67(3) 47, 147
section 67(4) 48, 147
section 67(5) 48, 147
section 67(6) 147

section 68 .... 148, 323, 324

section 69 .... 134, 148

section 70(2) 124, 135
section 70(3) 149

section 71(2) 124, 135

section 72 .... 132, 135, 149, 292, 336

section 73 .... 38, 39, 60, 95, 96, 259, 267, 272, 274, 308, 325

section 74 .... 35, 40, 95, 96, 268, 273

section 75 268

section 76 .... 269, 323
section 76(6) 270

section 77(1) 269
section 77(2) 269
section 77(3) 270
section 77(4) 269
section 77(5) 270
section 77(6) 270
section 78 270

section 79 270

section 80(1) 271
section 80(2) 261, 271
section 80(3)(b) 36, 98
section 80(6) 272

section 82 .... 271, 274, 275
section 82(1) 271
section 82(2) 271
section 82(4) 271, 275
section 82(5) 275

section 83 .... 19, 258, 259, 264

section 84 .... 259, 261, 262, 264, 273
section 84 272
section 84(a) 259, 261, 278
section 84(b) 26
section 84(c) 2611
section 84(d) 261
section 84(e) 261
section 84(f) 261
section 84(h) 262, 264

section 85(a) 262
section 85(d) 262
section 85(4) 271
section 85(5) 271

section 86 .... 264, 265
section 86(1) 264
section 86(2) 264

section 87 40

section 88 265
section 88(1) 264, 270
section 88(2) 265
section 88(3) 265, 270
section 88(4) 265, 270

section 89(2) 266

section 90 266

section 91 266

section 92 266

section 93(1) 267

section 94 262

section 96 273
section 96(1) 261, 273
section 96(2) 274
section 96(4) 274

section 97 261

section 99(2)(a) 274
section 99(2)(b) 274

section 100 274

section 101 274

section 102(1) 261

section 103 45

section 104 .... 10, 17, 26, 28-32, 56, 113, 164, 165, 170, 193, 197, 198, 199, 211, 238, 268, 241, 314
section 104(1)(a) 29
section 104(1)(b) 29
section 104(1)(c) 30
section 104(1)(d) 30
section 104(1)(f) 31
section 104(1)(g) 31
section 104(1)(h) 32
section 104(1)(i) 32
section 104(2) 32

section 105 257

section 106(1) 258

section 107 8
section 107(1)(b) 44
section 107(2)(a) 148
section 107(2)(f) 216
section 107(4) 121, 141
section 107(5) 149

section 108(1)(c) 306
section 108(1)(g) 18, 280

section 112(1) 311

section 113(2) 312
section 113(3) 312

section 115 312

section 116 312

section 118 311

section 120 309

section 123(3) 311

security in contracting 304
security measures 116, 118, 126, 133, 256, 294, 300, 301
security policy 277, 288, 301-304
Seniors Drug Profile 145, 146
severing 28, 33, 46, 47, 51, 52, 62-63
software 16, 34, 54, 102, 108, 110, 118, 119, 120, 124, 146, 287, 300, 304, 324
standardized diagnostic tests and assessments 76
statement of disagreement 95
storage facilities 51, 101, 120, 300, 303
storage media 282, 300
stripping 136
subpoena 8, 28, 204-205, 209, 212, 308, 309, 311
substitutional service 45
successor 213-214

T

taking reasonable steps 113
telecommunications system 45, 257
The Alberta Health Facilities Review Committee 204, 312
the date on which the health services provider became authorized to provide health services 13
theft 118, 213, 300
threat 114
threat and risk assessment 116, 288, 299, 302
time
  extension 35, 97
  limit 34-35
  period 53, 101
tracking systems 54, 102
training plan 134, 255
transitory records 44, 100, 280-281, 284

U

unauthorized access 114, 119, 186, 278, 280, 287, 300, 302
unauthorized collection 114, 133, 293, 296
unauthorized disclosure 114-115, 117, 294, 302
unauthorized modification 115
unauthorized use 114, 115, 116-117, 118, 278, 280, 302
unreasonably interfere with operations 40
use 176

V

virus 119, 120, 300, 303
Vital Statistics Act 213

W

warrant 8, 28, 204-205, 209, 212
Workers' Compensation Act 15
Workers' Compensation Board 4, 15, 162, 185

X

x-rays 11, 16, 26, 93, 286, 307